c5541abf-15ce-464f-b5d2-758395fcdf3e

Front-End- und Back-End-Server-Topologiehandbuch für Exchange Server 2003 und Exchange 2000 Server

Microsoft Corporation

Veröffentlicht: 12.12.06

Autor: Exchange Server-Dokumentationsteam

Kurzdarstellung

In diesem Handbuch wird die Front-End- und Back-End-Serverarchitektur und -topologie behandelt.

Kommentare? Senden Sie Ihr Feedback an folgende Adresse: exchdocs@microsoft.com.

Contents

Front-End- und Back-End-Server-Topologie unter Exchange Server 2003 und Exchange 2000 Server-Handbuch 9

Einführung in die Front-End- und Back-End-Topologien für Exchange Server 2003 und Exchange 2000 Server 9
- Vorausgesetzte Kenntnisse 10
- Neue Exchange Server 2003-Features für die Front-End- und Back-End-Architektur 10
- Kerberos-Authentifizierung 10
- RPC über HTTP 11
- Exchange Server 2003-Editionen 11
- Formularbasierte Authentifizierung 11
- Versionsunterstützung für Outlook Web Access 11

Übersicht über Front-End- und Back-End-Topologien 13

Vorteile der Front-End- und Back-End-Topologie 14
- Einzelner Namespace 14
- Verschieben der SSL-Verschlüsselung und -Entschlüsselung 15
- Sicherheit 15
- Verbesserter Zugriff auf Öffentliche Ordner und erweiterte Features 15
- Verbesserter IMAP-Zugriff auf Öffentliche Ordner 16
- Mehrere unterstützte Protokolle 16

Funktionsweise einer Front-End- und Back-End-Topologie 17

Integration mit IIS (Internet Information Services, Internet-Informationsdienste) 17

Remoteprozeduraufrufe in einem Umgebungsnetzwerk 17

Abhängigkeit von DSAccess 18

Systemaufsicht auf Front-End-Servern 18

Unterstützen von POP- und IMAP-Clients 20
- Authentifizierung für POP- und IMAP-Clients 20
- IMAP-Zugriff auf Öffentliche Ordner 21

Ausführen von SMTP für POP- und IMAP-Clients 21

Unterstützung für HTTP-Zugriff 22
- Suchen von Benutzerpostfächern 23
- Anmelden an Outlook Web Access 24

Vereinfachen des Outlook Web Access-URLs 25
Aktivieren des Features "Kennwort ändern" 26
Suchen von Öffentlichen Ordnern 26

Vereinfachen der Outlook Web Access-URL 31
Bevor Sie beginnen 31
Verfahren 32
Weitere Informationen 32

Authentifizierungsmechanismen für HTTP 33
Duale Authentifizierung 33
Pass-Trought-Authentifizierung 34
Authentifizierungsmethoden 34
Authentifizierung zwischen Client und Front-End-Server 35
Standardauthentifizierung 35
Formularbasierte Authentifizierung 36
Front-End/Back-End-Authentifizierung 36
Integrierte Authentifizierung 36
Standardauthentifizierung 37
Benutzeranmeldeinformationen 37

Remoteprozeduraufrufe (Remote Procedure Calls, RPCs) in der Exchange-Front-End- und Back-End-Topologie 37
Verlust von Features durch Platzierung eines Exchange-Front-End-Servers im Umkreisnetzwerk ohne RPC-Zugriff 38

Überlegungen zur Bereitstellung einer Front-End- und Back-End-Topologie 39
Keine Clusterbildung bei Front-End-Servern 39
Empfohlene Serverkonfigurationen und Einschätzungen 39
Lastenausgleich 40
Reduzieren der virtuellen Servererstellung 41

Verwenden von Firewalls in einer Front-End- und Back-End-Topologie 41
Anschlussfilterung 41
Quellanschluss im Vergleich zu Zielanschluss 42
Richtung der TCP-Verbindung 42
IP-Filterung 42
Anwendungsfilterung 42

Unterstützung für sichere Kommunikation zwischen Client und Front-End Server 43
Konfigurieren von SSL in einer Front-End- und Back-End-Topologie 43
SSL-Beschleuniger 44
SSL-Verschiebung 45
Formularbasierte Authentifizierung 46

Aktivieren der formularbasierten Authentifizierung bei Verwendung von SSL-Verschiebung 46

Bevor Sie beginnen 46
Verfahren 46
Weitere Informationen 47

Sichern der Kommunikation von Front-End-Servern zu anderen Servern 47
IP Security (IPSec) 47
IPSec-Protokolle 48
IPSec-Richtlinie 48
IPSec mit Firewalls und Filterrouter 49

Service Packs: Aktualisieren von Front-End- und Back-End-Servern 50
Überlegungen zur Aktualisierung von Outlook Web Access 50

Szenarien für die Bereitstellung einer Front-End- und Back-End-Topologie 51

Erweiterte Firewall in einem Umgebungsnetzwerk 52
Szenario 53
Setupanweisungen 53
Diskussion 54
Aspekte 54

Einrichten einer Front-End- und Back-End-Topologie mit einer erweiterten Firewall in einem Umgebungsnetzwerk 55
Bevor Sie beginnen 56
Verfahren 56

Front-End-Server hinter einer Firwall 57
Szenario 58
Setupanweisungen 58
Diskussion 58

Einrichten einer Front-End- und Back-End-Topologie mit einem Front-End-Server hinter einer Firewall 59
Bevor Sie beginnen 59
Verfahren 59

Webfarm mit einer Firewall 60
Szenario 60
Setupanweisungen 61
Diskussion 61
Aspekte 61

Einrichten einer Front-End- und Back-End-Topologie mit einer Webfarm hinter einer Firewall 61
Bevor Sie beginnen 62
Verfahren 62

Front-End-Server in einem Perimeternetzwerk 63
Szenario 63
Setupanweisungen 64
Diskussion 64
Aspekte 64

Einrichten einer Front-End- und Back-End-Topologie mit einem Front-End-Server in einem Perimeternetzwerk 65
Bevor Sie beginnen 66
Verfahren 66
Weitere Informationen 67

Konfigurieren von Exchange-Front-End-Servern 67

Festlegen eines Front-End-Servers 67
Bevor Sie beginnen 67
Verfahren 67
Weitere Informationen 68

Erstellen von virtuellen HTTP-Servern 68

Erstellen eines virtuellen Servers 69
Verfahren 69

Konfigurieren der Authentifizierung 70

Konfigurieren der Authentifizierung auf einem Front-End-Server 70
Bevor Sie beginnen 71
Verfahren 71

Konfigurieren eines Front-End-Servers als Standarddomäne 72
Konfigurieren von formularbasierter Authentifizierung für Exchange Server 2003 72

Konfigurieren eines Front-End-Servers als Standarddomäne 73
Bevor Sie beginnen 73
Verfahren 73

Konfigurieren der formularbasierten Authentifizierung in Exchange Server 2003 74
Bevor Sie beginnen 74
Verfahren 74

Zulassen einer E-Mail-Adresse als Anmeldebenutzername 75

Zulassen einer E-Mail-Adresse als Anmeldebenutzername 75
Bevor Sie beginnen 76
Verfahren 76

Deaktivieren von nicht mehr benötigten Diensten 76

URLSCan und IIS Lockdown-Assistent....78

Trennen und Löschen von Öffentlichen Informationsspeichern und Postfachspeichern....79

Konfigurieren von Netzwerklastenausgleich....80

Konfigurieren von SSL (Secure Sockets Layer)....80

Konfigurieren von SSL für POP3, IMAP4 und SMTP....81
Verfahren....81

Konfigurieren von SSL für HTTP....81
Verfahren....81
Weitere Informationen....82

Konfigurieren von SMTP auf dem Front-End-Server....82
E-Mail für interne Domänen....82
E-Mail für externe Domänen....82

Konfigurieren von DSAccess für Perimeternetzwerke....83
Deaktivieren NetLogon-Überprüfung....84
Deaktivieren der Ping-Funktion des Verzeichniszugriffs....84
Festlegen von Domänencontrollern und globalen Katalogservern....84

Vorgehensweise beim Deaktivieren der NetLogon-Überprüfung auf einem Front-End-Server....85
Bevor Sie beginnen....85
Verfahren....85

Deaktivieren der Pingausführung durch den Verzeichniszugriff....86
Bevor Sie beginnen....86
Verfahren....86

Hosten von mehreren Domänen....86
Methode eins: Erstellen zusätzlicher virtueller Server....87
Methode zwei: Erstellen zusätzlicher virtueller Verzeichnisse....89

Hinzufügen eines virtuellen Verzeichnisses auf einem virtuellen HTTP-Server in Exchange Server 2003....90
Verfahren....90
Weitere Informationen....91

Erstellen von virtuellen Verzeichnissen....91
Verfahren....91

Konfigurieren eines Back-End-Servers....92

Konfigurieren der Authentifizierung auf einem Back-End-Server....93

Erstellen und Konfigurieren von virtuellen HTTP-Servern auf Back-End-Servern 93
Methode eins: Konfigurieren von zusätzlichen virtuellen Servern 94
Methode zwei: Erstellen zusätzlicher virtueller Verzeichnisse 94

Konfigurieren von zusätzlichen virtuellen Servern auf einem Back-End-Server 95
Bevor Sie beginnen 95
Verfahren 95

Konfigurieren von Firewalls 96

Konfigurieren einer Internetfirewall 96
Konfigurieren von ISA Server 97

Konfigurieren einer Intranetfirewall 97
Erweiterter Firewallserver in einem Umgebungsnetzwerk 98
Front-End-Server in einem Umgebungsnetzwerk 99
Standardprotokolle 99
Active Directory-Kommunikation 100
DNS (Domain Name Service) 100
IPSec 101
RPCs (Remote Procedure Calls) 102
Beenden von RPC-Datenverkehr 102
Beschränken des RPC-Datenverkehrs 102

Front-End- und Back-End-Topologie - Prüfliste 103

Problembehandlung in einer Front-End- und Back-End-Topologie 109
Problembehandlungstools 109
Allgemeine Fehlerbehandlungsschritte 110
Anmeldungsfehlschläge 111
Fehlerbehandlung in Outlook Web Access 111

Copyright 111

Front-End- und Back-End-Server-Topologie unter Exchange Server 2003 und Exchange 2000 Server-Handbuch

Microsoft® Exchange Server 2003 und Microsoft Exchange 2000 Server unterstützen die Verwendung einer Serverarchitektur, bei der Serveraufgaben zwischen Front-End- und Back-End-Servern verteilt werden. In dieser Architektur nimmt ein Front-End-Server Anforderungen von Clients an und stellt diese über Proxy einem geeigneten Back-End-Server für die Verarbeitung zur Verfügung. Dieses Handbuch erläutert, wie Exchange Server 2003 und Exchange 2000 Server die Architektur mit Front-End- und Back-End-Server unterstützt. Weiterhin werden einige Front-End- und Back-End-Szenarien vorgestellt und Konfigurationsempfehlungen erteilt.

Hinweis:

Laden Sie das Front-End- und Back-End-Topologie unter Exchange Server 2003 und Exchange 2000 Server-Handbuch herunter, um das Dokument zu drucken oder offline zu lesen.

Einführung in die Front-End- und Back-End-Topologien für Exchange Server 2003 und Exchange 2000 Server

Microsoft® Exchange Server2003 und Microsoft Exchange2000 Server unterstützen den Einsatz einer Serverarchitektur, die Servertasks auf verschiedene Front-End- und Back-End-Server verteilt. In dieser Architektur nimmt ein Front-End-Server Anforderungen von Clients an und stellt diese über Proxy einem geeigneten Back-End-Server für die Verarbeitung zur Verfügung. In diesem Handbuch wird erläutert, wie Exchange Server 2003 and Exchange 2000 Server die Front-End- und Back-End-Serverarchitektur unterstützt. Das Handbuch beschreibt zudem verschiedene Front-End- und Back-End-Szenarien und enthält Empfehlungen für die Konfiguration.

Hinweis:

Ein Front-End-Server ist ein speziell konfigurierter Server unter Exchange Server 2003 oder Exchange 2000 Server. Ein Back-End-Server ist ein Server mit einer Standardkonfiguration. Zur Festlegung eines Servers als Back-End-Server ist keine Konfigurationsoption vorhanden. Der Begriff "Back-End-Server" bezieht sich auf alle

Server in einer Organisation, bei denen es sich nicht um Front-End-Server handelt, nachdem ein Front-End-Server in der Organisation eingeführt wurde.

Wichtig:

Die in diesem Handbuch enthaltenen Informationen beziehen sich auf Exchange Server 2003 oder höher und Exchange 2000 Server mit Service Pack 3 (SP3) oder höher. Wenn Sie frühere Versionen ausführen, ist die Aktualisierung auf Exchange Server 2003 oder Exchange 2000 Server mit Service Pack 3 (SP3) erforderlich, um die Vorteile der in diesem Handbuch beschriebenen Funktionen vollständig zu nutzen.

Vorausgesetzte Kenntnisse

Kenntnisse über Microsoft® Office Outlook® Web Access, Outlook Mobile Access, Exchange ActiveSync®, RPC über HTTP, Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol Version 3 (POP3) und Internet Message Access Protocol (IMAP) Version 4rev1 in einer Exchange-Standardumgebung sowie über grundlegende Exchange 2000 Server- und Microsoft Windows® Internet Information Services (IIS)-Konzepte werden in diesem Handbuch vorausgesetzt.

Neue Exchange Server 2003-Features für die Front-End- und Back-End-Architektur

Exchange Server 2003 baut auf der Front-End- und Back-End-Serverarchitektur auf und fügt neue Features und Funktionen hinzu, wie zum Beispiel die RPC über HTTP-Kommunikation, die Benutzern mit Outlook 2003-Clients den Zugriff auf Ihre Exchange-Informationen über das Internet ermöglicht. Mit der Standardversion von Exchange Server 2003 können Sie ebenfalls einen Server als Front-End-Server konfigurieren.

Kerberos-Authentifizierung

Eine Neuheit in Exchange Server 2003 ist die Fähigkeit des Exchange-Front-End-Servers, die Kerberos-Authentifizierung für HTTP-Sitzungen zwischen dem Front-End-Server und den jeweiligen Back-End-Servern zu verwenden. Auch wenn bei der Authentifizierung jetzt Kerberos eingesetzt wird, wird die Sitzung dennoch unter Verwendung von Klartext gesendet. Bei einem öffentlichen Netzwerk oder bei vertraulichen Daten ist es daher empfehlenswert, wenn Sie IPSec (Internet Protocol Security) zum Sichern der Kommunikation zwischen den Exchange-Front-End- und Back-End-Servern zu verwenden.

RPC über HTTP

Mit Exchange Server 2003 können Sie jetzt die RPC über HTTP-Funktion von Windows verwenden, um Benutzern, die Outlook 2003 ausführen, den Zugriff auf Unternehmensdaten über das Internet zu ermöglichen. Informationen zum Planen, Bereitstellen und Verwalten dieses neuen Exchange-Features finden Sie im Artikel Exchange Server 2003 RPC over HTTP Deployment Scenarios.

Exchange Server 2003-Editionen

Exchange Server 2003 ist in zwei Editionen verfügbar: Exchange Server 2003 Standard Edition und Exchange Server 2003 Enterprise Edition. Sie können beide Editionen als Front-End-Server in einer Front-End- und Back-End-Serverarchitektur konfigurieren.

Hinweis:

Exchange 2000 Server kann nur als Back-End-Server in einer Front-End- und Back-End-Konfiguration eingesetzt werden. Exchange 2000 Enterprise Server kann jedoch als Front-End-Server in einer Front-End- und Back-End-Konfiguration eingesetzt werden. Weitere Informationen zu den Unterschieden zwischen Exchange 2000 Server und Exchange 2000 Enterprise Server finden Sie im Microsoft Knowledge Base-Artikel 296614 über die Unterschiede zwischen der Standard und Enterprise Edition von Exchange 2000.

Formularbasierte Authentifizierung

Exchange Server 2003 enthält ein neues Authentifizierungsfeature für Ihre Outlook Web Access-Clients. Weitere Informationen zur Aktivierung dieses Features finden Sie unter Authentifizierungsmechanismen für HTTP.

Versionsunterstützung für Outlook Web Access

Zur Bereitstellung der neuen Exchange Server 2003-Version von Outlook Web Access ist die Installation von Exchange Server 2003 auf dem Front-End-Server und dem Back-End-Server erforderlich, zu dem die Benutzer eine Verbindung herstellen. Wenn Benutzer eine Verbindung zu einem Exchange 2003-Front-End- und Back-End-Server herstellen können Sie die Vorteile der folgenden Features nutzen:

- Formularbasierte Authentifizierung
- Antworten und Weiterleiten von Bereitstellungen in einem Öffentlichen Ordner über Outlook Web Access
- Integrierte Authentifizierung zwischen den Front-End- und Back-End-Servern

Verschiedene Kombinationen aus Exchange Server 2003, Exchange 2000 Server und Microsoft Exchange Server 5.5 bestimmen die Version von Outlook Web Access, die Ihre Benutzer verwenden können. In der folgenden Tabelle werden die Versionen von Outlook Web Access, auf die Benutzer basierend auf den auf dem Front-End- und Back-End-Servern installierten Exchange-Versionen zugreifen können, aufgelistet.

Für Benutzer verfügbare Outlook Web Access-Versionen

Front-End-Server	Back-End-Server	Outlook Web Access-Version
Exchange 5.5	Exchange 5.5	Exchange 5.5
Exchange 5.5	Exchange 2000	Exchange 5.5
Exchange 5.5	Exchange 2003	Nicht unterstützt
Exchange 2000	Exchange 5.5	Nicht unterstützt
Exchange 2000	Exchange 2000	Exchange 2000
Exchange 2000	Exchange 2003	Nicht unterstützt
Exchange 2003	Exchange 5.5	Nicht unterstützt
Exchange 2003	Exchange 2000	Exchange 2000
Exchange 2003	Exchange 2003	Exchange 2003

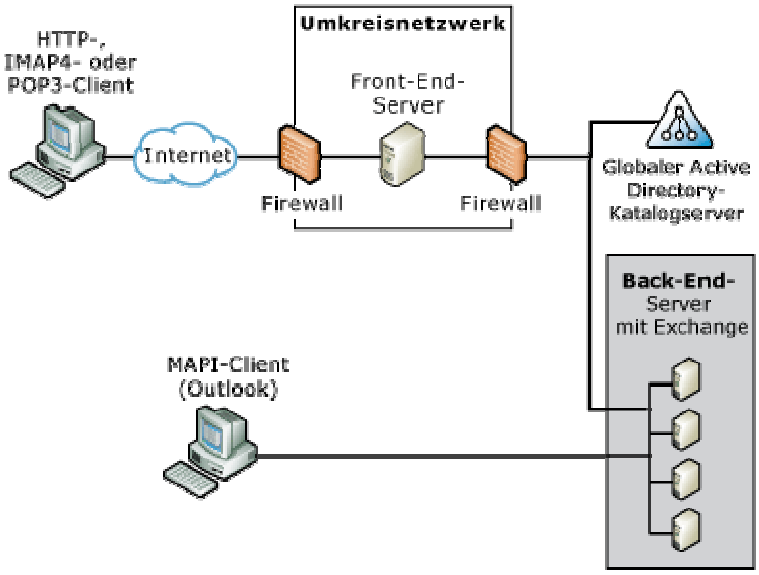
Die Exchange Server 2003-Version und Exchange 2000 Server-Version von Outlook Web Access unterscheiden sich erheblich von der Exchange Server 5.5-Version von Outlook Web Access. Die Exchange Server 5.5-Version von Outlook Web Access verwendet Active Server Pages (ASP) zur Kommunikation mit einem Exchange-Computer, der Collaboration Data Objects (CDO) 1.2 und MAPI verwendet. Die Anzahl der Clients, die gleichzeitig auf den Postfachspeicher zugreifen können, wird durch die MAPI-basierte Verbindung zum Exchange-Computer beschränkt.

Die Exchange Server 2003-Version und die Exchange 2000 Server-Version von Outlook Web Access setzen MAPI nicht für den Zugriff auf den Postfachspeicher ein und verwenden keine ASP-Seiten für Clientverbindungen. Für Verbindungen zur Web Access-Komponente verwenden diese Clients nach wie vor das Hypertext Transfer Protocol (HTTP). Der Internet Information Services (IIS)-Server, der die Outlook Web Access-Komponente hostet, verwendet den Microsoft Exchange-Informationsspeicherdienst für den Zugriff auf Messagingfunktionen. IIS empfängt Outlook Web Access-Clientanfragen als Proxy für Nachrichten zwischen einem Webclient und einem Exchange 2003-Server oder einem Exchange 2000-Server. Wenn der Server die Exchange 2003-Datenbank enthält, verwendet Outlook Web Access einen Hochgeschwindigkeitskanal für den Zugriff auf den Postfachspeicher. Wenn es sich bei dem Server um einen Front-End-Server handelt, sendet Outlook Web Access die Anfrage über HTTP an einen Back-End-Server.

Übersicht über Front-End- und Back-End-Topologien

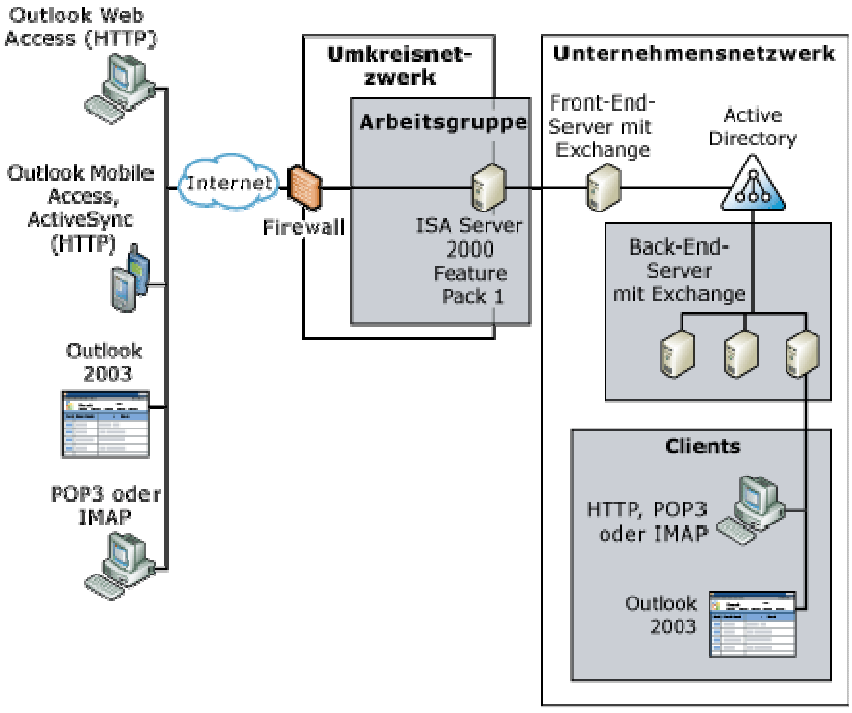
Die Abbildungen in diesem Thema beschreiben die Standardimplementierungen der Front-End- und Back-End-Serverarchitektur In der folgenden Abbildung wird eine einfache Front-End- und Back-End-Topologie in Exchange dargestellt.

Eine Front-End- und Back-End-Server-Architektur ohne erweiterte Firewall



In der folgenden Abbildung wird das empfohlene Szenario dargestellt, in dem eine erweiterte Firewall, wie zum Beispiel Microsoft® Internet Security und Acceleration (ISA) Server mit Service Pack1 (SP1) und Feature Pack1, zwischen dem Internet und dem Exchange-Front-End-Server eingesetzt wird.

Die empfohlene Exchange-Front-End- und Back-End-Server-Architektur



Vorteile der Front-End- und Back-End-Topologie

Die Front-End- und Back-End-Servertopologie sollte in Organisationen mit mehreren Server eingesetzt werden, die Ihren Mitarbeitern E-Mail-Zugriff über das Internet ermöglichen möchten. Zudem profitieren Organisationen, die Microsoft® Office Outlook® Web Access, POP, IMAP und RPC über HTTP in ihrem internen Netzwerk verwenden, ebenfalls von einer Front-End- und Back-End-Servertopologie.

Einzelner Namespace

Der Hauptvorteil der Front-End- und Back-End-Servertechnologie besteht in der Möglichkeit, einen einzelnen, konsistenten Namespace zu bereitzustellen. Sie können einen einzelnen Namspace für Benutzer für den Zugriff auf ihre Postfächer festlegen, zum Beispiel "https://mail" für Outlook Web Access. Ohne einen Front-End-Server muss jeder Benutzer den Namen des Servers kennen, auf dem sein Postfach gespeichert ist. Dieses Vorgehen kompliziert die Verwaltung und schränkt Ihre Flexibilität ein, weil Sie die Benutzer jedes Mal

informieren müssen, wenn Sie aufgrund von Umstrukturierungen innerhalb Ihrer Organisation Postfächer auf einen anderen Server verschieben müssen.

Bei einem einzelnen Namespace können Benutzer denselben URL oder dieselbe POP- und IMAP-Clientkonfiguration verwenden, selbst wenn Server hinzugefügt oder entfernt und Postfächer verschoben werden. Zudem wird mit dem Erstellen eines einzelnen Namespace sichergestellt werden, das der HTTPS-, POP- oder IMAP-Zugriff skalierbar bleibt, wenn Ihre Organisation wächst. Schließlich reduziert ein einzelner Namespace die für SSL-Verschlüsselung erforderliche Anzahl an Serverzertifikaten, da Clients SSL auf denselben Servers mit demselben Namespace verwenden.

Verschieben der SSL-Verschlüsselung und -Entschlüsselung

Clients wie Microsoft Office Outlook® 2003 oder Outlook Web Access, die über das Internet auf Ihren Exchange-Server zugreifen, sollten SSL (Secure Sockets Layer) für Verbindungen zu ihren Exchange-Servern verwenden, um ihre Daten vor unbefugtem Zugriff zu schützen. Die Verarbeitung von SSL-Datenverkehr kann jedoch eine erhebliche Belastung für einen Server darstellen. Die Front-End- und Back-End-Architektur erlaubt dem Front-End die Verarbeitung der SSL-Verschlüsselung und entlastet den Prozessor auf den Exchange-Back-End-Servern, deren Systemleistung für die Verarbeitung von E-Mail-Nachrichten dadurch erhöht wird. Weitere Verbesserungen können durch die Verwendung von SSL-Beschleunigern oder durch Verschieben der SSL-Verschlüsselung nach erweiterten Firewalls (wie z. B. ISA 2000 mit Service Pack 1 und Feature Pack 1) erzielt werden.

Sicherheit

Der Front-End-Server kann als einziger Zugriffspunkt an oder hinter einem Firewall positioniert werden, der so konfiguriert ist, dass eine Datenübertragung aus dem Internet nur am Front-End möglich ist. Da auf dem Front-End-Server keine Benutzerinformationen gespeichert werden, bietet dieser Server der Organisation eine zusätzliche Sicherheitsstufe. Weiterhin authentifizieren Front-End-Server Anfragen, bevor sie sie über Proxy weiterleiten. Dadurch schützen sie die Back-End-Server vor Denial-of-Service-Angriffen.

Verbesserter Zugriff auf Öffentliche Ordner und erweiterte Features

Ein Exchange-Front-End-Server erhöht die Robustheit beim Zugriff auf Öffentliche Ordner, da er den Status der Back-End-Server kennt und mehrere Verweise für den Zugriff auf Daten aus Öffentlichen Ordnern verwenden kann. Diese Daten beinhalten Systemdaten, wie zum Beispiel Frei/Gebucht-Informationen aus Kalendern. Weiterhin ermöglicht ein Front-End-Server unter Exchange Server 2003 Benutzern die Verwendung von Outlook Web Access,

um auf Bereitstellungen in Öffentlichen Ordnern zu antworten oder diese weiterzuleiten. Ohne einen Front-End-Server können Bereitstellungen in Öffentlichen Ordnern nur gelesen werden.

Verbesserter IMAP-Zugriff auf Öffentliche Ordner

Die IMAP-Protokollspezifikation ermöglicht einem Server, einen Client an einen anderen Server zu verweisen. Exchange unterstützt diese Verweisfunktion, wenn ein Informationsspeicher für Öffentliche Ordner auf einem bestimmten Server den angeforderten Inhalt nicht enthält und der Client an einen anderen Server verwiesen werden muss. Für diese Funktion müssen die Clients jedoch IMAP-Verweise unterstützen, was bei den meisten Clients nicht der Fall ist. (Der Pine-Client und das Pine-Toolkit der University of Washington unterstützen beispielsweise Verweise.)

Wenn ein nicht verweisfähiger IMAP-Client eine Verbindung über einen Front-End-Server herstellt, kann der Client auf die gesamte Öffentliche Ordner-Hierarchie zugreifen, da der Front-End-Server selbst alle Verweise automatisch verarbeitet. Dadurch wird der Verweis für den Client transparent. Weitere Informationen zu nicht verweisfähigen IMAP-Clients finden Sie in RFC (Request for Comments) 2221 und RFC 2193.

Mehrere unterstützte Protokolle

Die Front-End-Serverarchitektur bietet Unterstützung für RPC über HTTP, HTTP, POP und IMAP. Sie können ebenfalls SMTP auf dem Front-End-Server installieren, obwohl es bedeutende Unterschiede zwischen SMTP auf einem Front-End-Server oder auf einem Back-End-Server gibt.

Hinweis:

Das MAPI RPC (Remote Procedure Call)-Protokoll, das von Outlook im Nicht-RPC über HTTP-Modus verwendet wird, wird vom Front-End-Server nicht über Proxy zur Verfügung gestellt. Outlook bietet eine integrierte Unterstützung für Situationen, in denen Postfächer von einem Server zum anderen verschoben werden oder der Inhalt auf einem Server nicht vorhanden ist.

Funktionsweise einer Front-End- und Back-End-Topologie

Obwohl die generelle Funktion des Front-End-Servers darin besteht, Clientanfragen über Proxy an die richtigen Back-End-Server zu senden, richtet sich die genau Funktionalität eines Front-End-Servers nach dem Protokoll sowie nach den ausgeführten Tasks.

In diesem Abschnitt werden die Windows®- und Microsoft Exchange Server-Komponenten erörtert, die für das Verständnis der Funktionsweise einer Front-End- und Back-End-Topologie erforderlich sind. Achten Sie darauf, dass Sie die Funktionsweise dieser Komponenten in einer Front-End- und Back-End-Topologie erfassen, und bewerten Sie die Auswirkungen dieser Änderungen auf Ihre Organisation.

In diesem Abschnitt wird ebenfalls dargelegt, wie Front-End- und Back-End-Server die verschieden Clientprotokolle unterstützen.

Integration mit IIS (Internet Information Services, Internet-Informationsdienste)

Exchange speichert die Konfigurationsinformationen im Active Directory®-Verzeichnisdienst, wohingegen IIS diese Informationen in der Metabase speichert. Die Metabase ist eine lokale Konfigurationsdatenbank für Protokolle, die IIS unterstützen. Die Exchange-Systemaufsicht repliziert wichtige in Active Directory über den Exchange-System-Manager an der Metabase vorgenommene Änderungen in regelmäßigen Abständen. Sie können den Zeitpunkt der Konfigurationsreplikation in den Einträgen der Ereignisanzeige vom Metabase-Aktualisierungsdienst (MSExchangeMU) verfolgen Setzen Sie zur Anzeige der MSExchangeMU-Ereignisse auf der Registerkarte **Diagnoseprotokoll** in den Servereigenschaften die MSExchangeMU-Protokollierungsstufe auf **Minimal** oder höher.

Remoteprozeduraufrufe in einem Umgebungsnetzwerk

Wenn Sie Ihre Exchange-Front-End-Server in einem Umgebungsnetzwerk platzieren, achten Sie darauf, dass Remoteprozeduraufrufe (RPCs, Remote Procedure Calls) für den Zugriff auf Active Directory verwendet werden.

Hinweis:

Bei diesem Verfahren empfiehlt es sich, einen erweiterten Firewallserver (wie zum Beispiel ISA Server) anstelle des Front-End-Servers im Umgebungsnetzwerk einzusetzen. Weitere Informationen finden Sie unter Erweiterte Firewall in einem Umgebungsnetzwerk.

Remoteprozeduraufrufe werden von Internet-Informationsdiensten (IIS, Internet Information Services) zur Authentifizierung von Clients auf dem Front-End-Server verwendet.

Abhängigkeit von DSAccess

DSAccess ist eine freigegebene Exchange Server-Komponente, die auf Verzeichnisinformationen in einem Cache zugreift und diese speichert. Basierend auf Kriterien wie Active Directory-Sitekonfiguration und Active Directory-Serververfügbarkeit können Verzeichnisserver, die andere Exchange-Komponenten kontaktieren sollten, von DSAccess dynamisch erkannt werden. Exchange-Front-End-Server verwenden DSAccess, um zu ermitteln, welcher Server ein bestimmtes Benutzerpostfach, die SMTP (Simple Mail Transfer Protocol)-Adressen für ein bestimmtes Benutzerobjekt, die Server mit den Informationsspeichern für Öffentliche Ordner usw. enthält.

DSAccess verwendet das LDAP-Protokoll (Lightweight Directory Access Protocol) für die meisten Operationen. DSAccess verwendet jedoch nach wie vor RPCs zur Aktivierung des NetLogon-Dienstes für alle erkannten Domänencontroller und globalen Katalogserver.

Wenn Sie einen Front-End-Server in einem Umgebungsnetzwerk platzieren, in dem Sie den RPC-Datenverkehr zwischen dem Umgebungsnetzwerk und dem Unternehmensnetzwerk auf bestimmte Server beschränken möchten, schlägt NetLogon RPC über DSAccess auf Domänencontroller und globale Katalogserver möglicherweise fehl. Wenn dieser Fall eintritt, erkennt DSAccess, dass die RPC-Konnektivität lediglich blockiert ist und die Server nach wie vor verfügbar sind. DSAccess sendet jedoch weiterhin den NetLogon RPC, der die Systemleistung beeinträchtigen kann.

Wenn Sie die NetLogon RPC-Prüfung über DSAccess beenden möchten, können Sie einen Registrierungsschlüssel erstellen. Weitere Informationen zur Optimierung von DSAccess in einem Umgebungsnetzwerk finden Sie unter Konfigurieren von DSAccess für Perimeternetzwerke.

Systemaufsicht auf Front-End-Servern

Standardmäßig sind RPCs für die Ausführung der Exchange-Systemaufsicht auf einem Front-End-Server nicht mehr erforderlich. Die Komponenten der Systemaufsicht, die RPCs verwenden, werden auf Front-End-Server nicht mehr geladen. Diese Komponenten sind

daher bei der Festlegung eines Servers als Front-End-Server deaktiviert. Die folgende Liste bietet eine Kurzbeschreibung dieser Komponenten:

- **DSProxy**

  Der DSProxy-Dienst verweist MAPI-Clients (wie beispielsweise Microsoft® Office Outlook® 2002) an globale Katalogserver für Suchläufe in der globalen Adressliste. DSProxy gewährt MAPI-Clients mit älteren Outlook-Versionen ebenfalls Zugriff auf Active Directory. DSProxy wird auf Front-End-Servern nicht mehr ausgeführt. Der Front-End-Server kann daher nicht mehr feststellen, welcher Back-End-Server ein Postfach eines MAPI-Clients enthält. Aus diesem Grund kann ein MAPI-Client nicht mehr an den Front-End-Server verwiesen werden, um den Back-End-Server des Benutzers zu ermitteln und die Anfrage anschließend an den gewünschten Server weiterzuleiten.

  Hinweis:

  Wenn Sie DSProxy auf dem Front-End-Server zur Weiterleitung von MAPI-Clientanfragen aktivieren möchten, installieren Sie Exchange 2000 Server Service Pack 3 (SP3), und erstellen Sie den Registrierungsschlüssel. Weitere Informationen hierzu finden Sie im Microsoft Knowledge Base-Artikel 319175 mit Erläuterungen zu XADM: Die Überprüfung von Namensabfragen auf einem Front-End-Computer unter Exchange können nicht ausgeführt werden. Beachten Sie, dass der Client RPC-Zugriff auf den Front-End-Server benötigt, um diese Verweise zu erhalten. Der Front-End-Server muss zudem RPC-Zugriff auf die Domänencontroller haben.

- **Empfängeraktualisierungsdienst**

  Der Empfängeraktualisierungsdienst aktualisiert Empfänger im Verzeichnis, um Adresslisten oder die Empfängerrichtlinien des Proxy abzugleichen. Der Empfängeraktualisierungsdienst wird nicht mehr auf Front-End-Servern ausgeführt. Stellen Sie daher sicher, dass keiner Ihrer Front-End-Server zur Ausführung des Empfängeraktualisierungsdienstes konfiguriert ist. Überprüfen Sie hierzu im Exchange-System-Manager unter **Empfänger** die Eigenschaften aller Empfängeraktualisierungsdienste, und stellen Sie sicher, dass im Feld **Exchange-Server** kein Front-End-Server aufgeführt ist.

- **Erstellen des Offlineadressbuchs (OABGen)**

  OABGen erstellt das Offlineadressbuch. Ohne den OABGen-Dienst werden Offlineadressbücher von Front-End-Servern nicht mehr erstellt.

- **Gruppenabruf**

  Die Systemaufsicht verwendet die Gruppenabruffunktion, um sicherzustellen, dass der lokale Computer Mitglied der Domain Exchange Server-Gruppe bleibt. Die Systemaufsicht ruft die Domain Exchange Servers-Gruppe ab und fügt den lokalen Computer der Gruppe erneut zu, wenn dieser kein Mitglied mehr ist. Front-End-Server führen diese Funktion nicht mehr aus.

- **Postfachverwaltung**

  Der Postfachverwaltungsdienst startet und beendet die Bereinigung des Postfachs gemäß den in den Empfängerrichtlinien festgelegten Einstellungen. Die Postfachverwaltungsfunktion wird auf Front-End-Servern nicht mehr ausgeführt.

- **Frei/Gebucht (madfb.dll)**

  Der Frei/Gebucht-Dienst verwaltet die Termine der Benutzer. Dieser Dienst wird auf Front-End-Servern nicht mehr ausgeführt.

Unterstützen von POP- und IMAP-Clients

Wenn Sie einen Front-End-Server verwenden, werden den Benutzern die Namen der Server nicht angezeigt, die als Hosts für Postfächer fungieren. Clientcomputer stellen eine Verbindung zu den Front-End-Servern her, die sich einen Hostnamen teilen. Das Verschieben von Benutzern zwischen Servern ist daher für alle Benutzer nachvollziehbar und bedarf keiner erneuten Konfiguration der Clientcomputer.

Beim Anmelden sendet ein POP- oder IMAP-Client eine Anmeldeanfrage an den Front-End-Server, die den Namen des Postfachs enthält, auf das zugegriffen werden soll. Der Front-End-Server authentifiziert den Benutzer und verwendet Active Directory, um festzulegen, welcher Back-End-Server das Postfach des Benutzers enthält. Der Front-End-Server stellt die Anmeldeanfrage dem jeweiligen Back-End-Server über Proxy zur Verfügung. Der Back-End-Server sendet dann das Ergebnis der Anmeldung zurück an den Front-End-Server, der wiederum diese Ergebnisse an den Client zurückgibt. Nachfolgende POP- und IMAP-Befehle werden entsprechend ausgeführt.

Hinweis:

Für die Weiterleitung von E-Mail durch POP- und IMAP-Clients muss SMTP verfügbar sein. Sie können SMTP auf einem Front-End-Server installieren oder einen separaten SMTP-Server einrichten. Die Weiterleitung von E-Mail durch SMTP auf einem Front-End-Server funktioniert genau so wie auf anderen Exchange-Servern. Weitere Informationen zum Konfigurieren von SMTP auf einem Front-End-Server finden Sie unter Konfigurieren von Exchange-Front-End-Servern.

Authentifizierung für POP- und IMAP-Clients

POP- und IMAP-E-Mailclients senden Benutzer- und Kennwortinformationen in unverschlüsseltem Text. Wenn der Zugriff auf den Front-End-Server über das Internet möglicht ist, sollten Sie SSL so konfigurieren, dass die Authentifizierungsinformationen des Benutzers nicht unverschlüsselt über das Internet weitergeleitet werden.

IMAP-Zugriff auf Öffentliche Ordner

Wenn ein nicht verweisfähiger IMAP-Client eine Verbindung zu einem Back-End-Server herstellt, kann er nur auf Öffentliche Ordner zugreifen, die über ein Replikat auf dem Stammserver des Benutzers verfügen. Für den Zugriff auf Öffentliche Ordner mit Replikaten auf anderen Servern muss ein IMAP-Client verweisfähig sein. Ein verweisfähiger Client leitet spezielle Befehle an einen IMAP-Server weiter, um eine Liste mit den für den Client verfügbaren Öffentlichen Ordnern zu erstellen. Wenn der Clientcomputer einen Öffentlichen Ordner anfordert, der nicht über ein lokales Replikat verfügt, antwortet der Server auf die Clientanfrage mit einem Verweis-URL, der den Namen des Servers mit dem Öffentlichen Ordner enthält. Anschließend stellt der verweisfähige IMAP-Clientcomputer eine neue Verbindung zu diesem Server her, um die entsprechenden Informationen abzurufen.

In einer Front-End- und Back-End-Topologie fungiert der Front-End-Server jedoch als verweisfähiger Client, so dass IMAP-Clients, die eine Verbindung zum Front-End-Server herstellen, keine Unterstützung für Verweise bieten müssen. Der Front-End-Server übernimmt die Verweisfunktionalität für diese Clients. Verweisfähige Clientanfragen werden übersichtlich ihrem jeweiligen Gegenstück zugeordnet, wobei die gesamte Liste mit verfügbaren Öffentlichen Ordnern einem nicht verweisfähigen Client zur Verfügung gestellt wird. Wenn der Front-End-Server eine Verweisantwort von Back-End-Server empfängt, leitet er diese Antwort nicht zurück zum Client. Stattdessen folgt er dem Verweis für den Client und stellt eine Verbindung zum jeweiligen Back-End-Server her, der über die Daten verfügt. Der Back-End-Server antwortet anschließend mit dem angeforderten Element, das der Front-End-Server an den Client weiterleitet.

Ausführen von SMTP für POP- und IMAP-Clients

POP- und IMAP-Protokolle werden nur für den Empfang von Nachrichten verwendet. SMTP muss auf dem Front-End-Server konfiguriert werden, damit POP- und IMAP-Clients Nachrichten bereitstellen können. SMTP muss nicht auf dem Exchange-Front-End-Server ausgeführt werden, sondern auf beliebigen Servern, die als dediziertes SMTP-Gateway konfiguriert sind.

Wichtig:

Wenn Sie SMTP auf dem Front-End-Server ausführen und diesen für den Empfang von eingehenden Nachrichten (Nachrichten für Ihre Domänen) konfigurieren, müssen Sie einen Postfachspeicher auf dem Front-End-Server einrichten. Diese Postfachspeicher muss keine Postfächer enthalten. Stellen Sie einen Postfachspeicher auf dem Front-End-Server bereit, da alle Unzustellbarkeitsberichte über den Postfachspeicher zur Formatierung weitergeleitet werden müssen.

Um SMTP so zu konfigurieren, dass POP- und IMAP-Clients Nachrichten an externe Domänen weiterleiten können, müssen Sie Relay zulassen.

Standardmäßig lässt Exchange Relay nur für authentifizierte Clients zu. Die Beibehaltung dieses Standards wird empfohlen. Clients, wie zum Beispiel Microsoft Outlook Express 6.0 und Microsoft® Office Outlook® 2003 sowie frühere Versionen von Outlook Express und Outlook unterstützen neben der SMTP-Authentifizierung die TLS (Transport Layer Security)-Verschlüsselung.

Relay sollte wie folgt nicht zugelassen werden:

- Anonymes Relay sollte für alle IP-Adressen nicht zugelassen werden. Wenn Ihr Front-End-Server mit dem Internet verbunden ist, könnten bei zugelassenem Relay beliebige Benutzer über das Internet Ihren Server zum Senden von Nachrichten verwenden.
- Relay sollte für bestimmte Client-IP-Adressen nicht zugelassen werden. Selbst wenn Sie mit dem Subnet, über das die Clients Nachrichten senden, vertraut sind, ist es in einer Internetumgebung schwierig, bestimmte IP-Adressen zu ermitteln.

Hinweis:

Wenn der Front-End-Server als Bridgeheadserver zwischen Ihrem Unternehmen und dem Internet eingesetzt wird, sollte der Server im Internet, der E-Mail-Nachrichten für Ihre Domänen akzeptiert, eingehende Nachrichten auf Viren überprüfen.

Hinweis:

Weitere Informationen finden Sie im Transport- und Routing-Handbuch für Exchange Server 2003.

Unterstützung für HTTP-Zugriff

Unabhängig davon, ob HTTP-Anfragen von einem Browser oder einem spezialisierten Client erstellt wurden, werden Sie vom Clientcomputer zum Front-End-Server gesendet. Der Front-End-Server verwendet Active Directory, um zu ermitteln, an welchen Back-End-Server die Anfrage über Proxy weitergeleitet werden soll.

Nach Auswahl des richtigen Back-End-Servers leitet der Front-End-Server die Anfrage an den Back-End-Server weiter. Neben den speziellen Headerinformationen, in denen angegeben wird, dass die Anfrage an einen Front-End-Server weitergeleitet wurde, entspricht die Anfrage nahezu der ursprünglichen Anfrage des Clients. Vor allem bleibt der HTTP-Hostheader, der dem Namen des Front-End-Servers entspricht, an den die Anfrage gesendet wurde (d. h. der Hostname oder vollständig qualifizierte Domänenname, den der Benutzer im Browser eingegeben hat), unverändert. Der Front-End-Server kontaktiert den Back-End-Server mit dem Hostnamen des Back-End-Servers (z. B. backend1), aber im HTTP-Header der Anfrage sendet der Front-End-Server den vom Client verwendeten Hostheader, z. B. www.adatum.com. Die Hostheadereinstellungen gewährleisten, dass der richtige virtuelle

Exchange-Back-End-Server die Anfrage verarbeitet. Weitere Informationen zum Konfigurieren von virtuellen Servern auf einem Back-End-Server finden Sie unter Konfigurieren eines Back-End-Servers.

Bei HTTP-Anfragen kontaktiert der Front-End-Server den Back-End-Server immer über TCP-Anschluss 80 (HTTP-Standardanschluss), unabhängig davon, ob der Client den Front-End-Server über Anschluss 80 oder 443 (SSL-Anschluss) kontaktiert hat. Dies bedeutet Folgendes:

- Virtuelle HTTP-Server auf dem Exchange-Front-End-Server stehen nur am Anschluss 80 (HTTP) oder 443 (HTTPS) zur Verfügung.

  Hinweis:

  Außer den Anschlüssen 80 und 443 können keine anderen Anschlüsse für virtuelle HTTP-Server auf Exchange-Front-End-Servern verwendet werden.

- SSL-Verschlüsselung wird zwischen Front-End- und Back-End-Servern nie eingesetzt, obwohl der Client diese Funktion zur Kommunikation mit dem Front-End-Server verwenden sollte.

- Virtuelle HTTP-Server, die sich von anderen Server nur durch die Anschlussnummer unterscheiden, werden in einer Front-End- und Back-End-Topologie nicht unterstützt. Wenn ein Back-End-Server über einen virtuellen HTTP-Server verfügt, der Anschluss 8080 überwacht, kann ein Client nur dann auf diesen Back-End-Server zugreifen, wenn er direkt auf diesen Back-End-Server verwiesen wird (Beispiel: http://backend1:8080/data). Ein mit dem Front-End-Server verbundener Client kann auf diese Daten nicht zugreifen.

Der Back-End-Server verarbeitet die HTTP-Anfrage vom Front-End-Server, und die Antwort wird unverändert über den Front-End-Server zurück zum Client gesendet. Der gesamte Vorgang ist für den Client, der nur mit dem Front-End-Server interagiert, nicht sichtbar. Der Client weiß nicht, wie die Anfrage intern verarbeitet wird.

Suchen von Benutzerpostfächern

Wenn Sie den Zugriff auf Postfachordern über HTTP ermöglichen möchten, müssen Sie sowohl auf den Exchange-Front-End- als auch auf den Back-End-Servern ein virtuelles Verzeichnis einrichten, dass auf die Postfächer verweist.

Hinweis:

Benutzerpostfächer können nicht auf dem Front-End-Server gespeichert werden.

Beim Installieren von Exchange wird das virtuelle Verzeichnis "Exchange" auf dem virtuellen Standardserver erstellt. Dieses Verzeichnis verweist auf die SMTP-Standarddomäne der Exchange-Organisation. Beim Konfigurieren zusätzlicher virtueller Verzeichnisse auf dem Front-End-Server über den Exchange-System-Mananger können Sie den SMTP-

Domänennamen auswählen. In Exchange 2000 Server SP3 und Exchange Server 2003 müssen Benutzer, die eine Verbindung zu diesem virtuellen Server herstellen, über eine E-Mail-Adresse der SMTP-Proxyadressliste ihres Active Directory-Objekts mit derselben Domäne verfügen. In Exchange Server 2003 SP1 können Benutzer die SMTP-Domäne überschreiben, indem sie im URL die SMTP-Adresse angeben (für die explizite Anmeldung) oder sich lediglich implizit anmelden. Weitere Informationen finden Sie unter "Anmelden an Outlook Web Access" weiter unten in diesem Thema.

Im Dialogfeld zur Auswahl der SMTP-Domäne stellt die Domänenliste eine Auflistung der Domänen dar, für die Empfängerrichtlinien gelten. Aus diesem Grund werden möglicherweise doppelte Einträge angezeigt. Dabei ist es unerheblich, welchen der doppelten Einträge Sie auswählen.

Wenn der Front-End-Server eine Anfrage an eine Position im Postfachspeicher erkennt (basierend auf den Einstellungen des virtuellen Servers bzw. virtuellen Verzeichnisses), kontaktiert er einen globalen Active Directory-Katalogserver in der Domäne unter Verwendung von LDAP (Lightweight Directory Access Protocol) und ermittelt, welcher Back-End-Server das Postfach des Benutzers enthält.

Anmelden an Outlook Web Access

Benutzer können sich implizit oder explizit an Outlook Web Access anmelden.

Implizite Anmeldung

Wenn der Front-End-Server zur Authentifizierung konfiguriert ist, können Benutzer auf ihre Postfächer zugreifen, indem Sie den Benutzernamen in der Anfrage auslassen und über ihren Browser auf das virtuelle Postfachverzeichnis verweisen. Der Standard-URL ist https://*<server>*/exchange/. Nach der Authentifizierung des Benutzers werden die Authentifizierungsinformationen für die Suche nach dem Postfach verwendet, das mit dem Benutzer in Active Directory und dem Back-End-Server, auf dem sich das Postfach befindet, verknüpft ist. Der URL wird mit dem Benutzernamen aktualisiert und an den richtigen Back-End-Server weitergeleitet. Dieses Verfahren wird als implizite Anmeldung bezeichnet. Die implizite Anmeldung ist bei der Anmeldung an Outlook Web Access hilfreich. Spezialisierte HTTP-Clients verwenden die implizite Anmeldung normalerweise nicht.

Exchange 2000 Server SP3 und Exchange Server 2003

Bei der impliziten Anmeldung wird die im virtuellen HTTP-Verzeichnis angegebene SMTP-Domäne verwendet, um den Benutzer zu identifizieren. Benutzer, die eine Verbindung zu diesem virtuellen Server herstellen, müssen daher in ihrer SMTP-Proxyadressliste im Active Directory-Objekt über eine E-Mail-Adresse mit derselben Domäne verfügen.

Exchange Server 2003 SP1

Die implizite Anmeldung ist nicht mehr ausschließlich von der angegebenen SMTP-Domäne abhängig. Alle Benutzerinformationen können aus der jeweiligen Anmeldung abgeleitet werden. Benutzer können beliebige virtuelle Exchange-Postfachverzeichnis für den Zugriff auf ihre E-Mail-Nachrichten verwenden.

Explizite Anmeldung

Zum Herstellen eine Verbindung zu Outlook Web Access stehen einige wenige URLs zur Verfügung. Der Standard-URL ist https*://<server>/*exchange*/<benutzername>*/. Der Zugriff auf Outlook Web Access mit diesem URL wird als explizite Anmeldung bezeichnet.

Explizite Anmeldung ist erforderlich, wenn der Front-End-Server nicht zur Authentifizierung von Benutzern konfiguriert ist (weitere Informationen zur Authentifizierung finden Sie unter Authentifizierungsmechanismen für HTTP) oder ein Benutzer mit Zugriffsberechtigung auf ein Postfach einer anderen Person zugreift, zum Beispiel bei stellvertretenden Benutzern.

Exchange 2000 Server SP3 und Exchange Server 2003

Wenn ein Front-End-Server eine explizite Anmeldeanforderung vom Client erhält, wird der Benutzername aus dem URL extrahiert und mit dem SMTP-Domänennamen kombiniert, der mit dem virtuellen Verzeichnis oder dem virtuellen Server verknüpft ist, um eine vollständig qualifizierte SMTP-Adresse zu erhalten. Der Front-End-Server sucht diese Adresse in Active Directory und legt fest, welcher Back-End-Server über das mit dieser Adresse verknüpften Postfach verfügt. Anschließend leitet der Front-End-Server die Anfrage an den Back-End-Server weiter, der wiederum die Anfrage über den Front-End-Server an den Client zurückgibt.

Exchange Server 2003 SP1

Der Benutzer kann die im virtuellen Postfachverzeichnis konfigurierte SMTP-Domäne überschreiben, indem er die SMTP-Adresse im URL selbst angibt. Beispiel: https://<server>/exchange/username@domain.com. Wurde keine SMTP-Domäne angegeben, wird die SMTP-Domäne aus dem virtuellen Verzeichnis verwendet.

Sie können den Zugriff auf Outlook Web Access für bestimmte Benutzer verweigern, indem Sie die Verwendung des HTTP-Protokolls durch diese Benutzer nicht erlauben. Wenn Sie die Protokolleinstellungen für Active Directory-Benutzer und -Computer ändern möchten, verwenden Sie die Registerkarte **Exchange - Erweitert** in den Eigenschaften der Benutzer.

Vereinfachen des Outlook Web Access-URLs

Häufig fragen Benutzer nach einem vereinfachten URL für den Zugriff auf ihre Postfächer. Ausführliche Anweisungen zum Vereinfachen des Outlook Web Access-URLs finden Sie unter Vereinfachen der Outlook Web Access-URL.

Aktivieren des Features "Kennwort ändern"

Wenn Sie Outlook Web Access verwenden, können Sie das Feature zum Ändern des Kennworts in IIS verwenden, um die folgenden Aktionen auszuführen:

- Warnen von Benutzern vor dem Ablauf ihrer Kennwörter
- Benutzern die Verwendung der Schaltfläche **Optionen** in Outlook Web Access zum Ändern von Kennwörtern ermöglichen.

Beachten Sie, dass Sie bei Verwendung des Features zum Ändern des Kennworts ebenfalls SSL zwischen Clients und dem Front-End-Server verwenden müssen, um das Kennwort während der Übertragung zu sichern. Weiterhin müssen Sie den virtuellen Verzeichnisnamen **IISAdmPwd** auf den Front-End- und Back-End-Servern erstellen, um die Anfragen zum Ändern des Kennworts zu verarbeiten.

Hinweis:

SSL ist nur dann auf einem Back-End-Server erforderlich, wenn sich die Benutzer direkt mit dem Back-End-Server verbinden sollen. Erinnern Sie sich daran, dass Front-End-Server SSL nicht für Verbindungen zu Back-End-Servern verwendet werden können. Wenn Sie SSL daher auf dem Back-End-Server benötigen, überprüfen Sie, ob Sie SSL für die folgenden Verzeichnisse nicht benötigen und Front-End-Server diese nach wie vor kontaktieren können: Exchange, Public, ExchWeb, Exadmin und alle virtuellen Stammverzeichnisse für Postfächer und Öffentliche Ordner.

Weitere Informationen zum Konfigurieren des Features "Kennwort ändern" finden Sie im Microsoft Knowledge Base-Artikel 327134, "XCCC: SO WIRD'S GEMACHT: Verwenden der Funktion zum Ändern von Kennwörtern in Outlook Web Access".

Weitere Informationen zum Konfigurieren von SSL finden Sie unter Unterstützung für sichere Kommunikation zwischen Client und Front-End Server.

Suchen von Öffentlichen Ordnern

Die Konfiguration von virtuellen Verzeichnissen für Postfächer entspricht derjenigen von virtuellen Verzeichnissen für alle Öffentliche Ordner-Strukturen, auf die über HTTP vom Front-End-Server aus zugegriffen werden muss.

Bei der Installation von Exchange wird das virtuelle Verzeichnis "public" auf dem virtuellen Exchange-HTTP-Standardserver erstellt, um Zugriff auf die standardmäßige (Zugriff über MAPI) Öffentliche Ordner-Struktur zu erteilen. Beim Erstellen von Öffentliche Ordner-Strukturen (zum Beispiel für Hostanwendungen) müssen Sie ebenfalls virtuelle Verzeichnisse im Exchange-System-Manager erstellen, um diese Strukturen über HTTP anzuzeigen. Auf allen Front-End- und Back-End-Servern, die die Öffentliche Ordner-Struktur hosten, müssen die virtuellen Verzeichnisse identisch sein.

Eine an einen URL in einer Öffentliche Ordner-Struktur gerichtete Anfrage wird beim Zugriff auf die standardmäßige (Zugriff über MAPI) Öffentliche Ordner-Struktur anders verarbeitet, als wenn der Zugriff auf allgemeine Ordner (auch als Anwendungen mit Hierarchien auf der obersten Ebene oder Nicht-Mapi-Hierarchien auf der obersten Ebene bezeichnet) erfolgt.

Der Zugriff auf Öffentliche Ordner hat zwei Ziele:

- **Verfügbarkeit** Wenn sich Daten in einem Öffentlichen Ordner von Exchange 2000 Server oder Exchange Server 2003 an einer beliebigen Stelle innerhalb der Exchange-Organisation befinden und der Zugriff über HTTP erfolgt, sind sie für den Benutzer verfügbar.
- **Konsistenz** So lange der Server verfügbar und der Benutzer authentifiziert ist, übernimmt derselbe Öffentliche Ordner-Server alle Anfragen von diesem Benutzer. Authentifizierten Benutzern werden immer dieselben Daten angezeigt, wenn sie auf die Öffentliche Ordner-Strukturen über den Front-End-Server zugreifen (einschließlich der Statusmeldungen über gelesene oder nicht gelesene Nachrichten, die auf einzelnen Servern gespeichert sind und zwischen den Öffentliche Ordner-Servern nicht repliziert werden). Damit ist sichergestellt, dass authentifizierte Benutzer an denselben Öffentliche Ordner-Server verwiesen werden. Die Tatsache, dass Benutzer immer denselben Bank-End-Server erreichen, ist ebenfalls für serverbasierte Anwendungen von Bedeutung, die den Sitzungsstatus beibehalten, wie zum Beispiel einige Versionen von ASP (Active Server Pages).

Verweise auf Öffentliche Ordner

In Exchange können Sie die Replikation von Öffentlichen Ordnern auf einer Pro-Ordner-Basis konfigurieren. Die aktuelle Hierarchie für Öffentliche Ordner-Strukturen sind auf allen Öffentliche Ordner-Servern von Exchange in der Organisation enthalten, wogegen der jeweilige Inhalt möglicherweise nicht verfügbar ist. Diese Informationen werden nicht in Active Directory gespeichert, sondern als Ordnereigenschaft im Informationsspeicher für Öffentliche Ordner verwaltet. Eine besondere Vorgehensweise ist daher erforderlich, wenn der vom Front-End-Server ausgewählte Back-End-Server den vom Client angeforderten Inhalt des Ordners nicht enthält.

In der folgenden Abbildung wird die Weiterleitung von Verweisen auf Öffentliche Ordner über einen Front-End-Server dargestellt.

Verweis auf einen Öffentlichen Ordner über einen Front-End-Server

1d21662d-c828-4409-8099-ffe0d1a1df53

1. Ein HTTP-Client authentifiziert sich am Front-End-Server und fordert /public/PublicFolder2 an.

2. Der Front-End-Server authentifiziert den Benutzer bei Active Directory und fordert den Speicherort des standardmäßigen Informationsspeichers für Öffentliche Ordner des Benutzers an.
3. Active Directory gibt dem Front-End-Server an, dass es sich bei dem standardmäßigen Informationsspeicher für Öffentliche Order des Benutzers um Server1 handelt.
4. Der Front-End-Server sendet die Clientanfrage an Server1.
5. Server1 teilt dem Front-End-Server mit, dass er nicht über den Inhalt /public/PublicFolder2 verfügt, verweist jedoch auf Server2 und Server3.
6. Der Front-End-Server führt einen Hashalgorithmus bei den Servern mit diesem Inhalt aus (in diesem Fall Server2 und Server3). Das Ergebnis dieses Hashalgorithmus ist in diesem Fall Server2, so dass der Front-End-Server die Anfrage an Server2 weiterleitet.

   Hinweis:

   Ein Hashalgorithmus wendet eine vorgegebene Zahlenfolge (in diesem Fall das Sicherheitskürzel des Benutzers) an, um eine Position auf einer Liste zu erzeugen. Sämtliche Eingaben können nun über die so erzeugte Liste verteilt werden.
7. Server2 gibt den Inhalt /public/PublicFolder2 an den Front-Server weiter, der den Inhalt an den HTTP-Client sendet.

Die Öffentliche Ordner-Standardstruktur (MAPI)

Wenn ein Client auf die Öffentliche Ordner-Standardstruktur in Outlook Web Access zugreift, erfolgt dies, um die Parität der MAPI-Clients, wie zum Beispiel Outlook, beizubehalten. Jeder Postfachspeicher ist mit einem bestimmten Informationsspeicher für Öffentliche Ordner an einer beliebigen Position in der Organisation verknüpft (manchmal auf demselben Server wie der Postfachspeicher, manchmal auf einem dedizierten Server für Öffentliche Ordner). Der mit dem Postfachspeicher des Benutzers verknüpfte Informationsspeicher für Öffentliche Ordner ist der Speicher, der die Öffentliche Ordner-Hierarchie (Struktur) in Outlook darstellt.

Wenn ein Benutzer einen Öffentlichen Ordner in der Öffentliche Ordner-Standardstruktur über HTTP anfordert, authentifiziert der Front-End-Server den Benutzer und sucht ihn in Active Directory, um zu ermitteln, welcher Öffentliche Speicher mit dem Postfachspeicher des Benutzers verknüpft ist. Der Front-End-Server leitet die Anfrage anschließend an den Öffentliche Ordner-Server des Benutzers weiter.

Wenn der Front-End-Server nicht zur Authentifizierung des Benutzers konfiguriert ist, findet bei Anfragen für Öffentliche Ordner kein Lastenausgleich statt.

Allgemeine Öffentliche Ordner-Strukturen

Standardserver für Öffentliche Ordner-Strukturen sind aufgrund ihres MAPI-Ursprungs mit Postfachspeichern verknüpft. Allgemeine Öffentliche Ordner-Strukturen verfügen nicht über eine derartige Verknüpfung. Anfragen nach Ordnern in allgemeinen Öffentliche Ordner-Strukturen werden daher etwas anders als Anfragen nach Ordnern in der Öffentlichen Ordner-Standardstruktur verarbeitet.

Wenn ein Client eine Anfrage für den Zugriff auf eine allgemeine Öffentliche Ordner-Struktur stellt, kontaktiert der Front-End-Server zunächst Active Directory, um eine Liste aller Server unter Exchange 2000 Server oder Exchange Server 2003 in der Organisation abzurufen, die ein Replikat dieser speziellen allgemeinen Öffentliche Ordner-Struktur haben, auf die der Client zugreift.

Hinweis:

Allgemeine Öffentliche Ordner-Strukturen sind in Exchange Server 5.5 nicht verfügbar.

Der Front-End-Server verwendet anschließend das Authentifizierungstoken in einem Hashalgorithmus für die Serverliste, um sicherzustellen, dass

- Benutzer auf die verfügbaren Server verteilt werden.
- einzelne Benutzeranfragen unabhängig vom verwendeten Client immer von demselben Back-End-Server verarbeitet werden.

Hinweis:

Wenn Sie einen Back-End-Server hinzufügen oder löschen, ändert sich das Ergebnis des Hashalgorithmus, und Benutzer werden möglicherweise an einen anderen Server weitergeleitet. Weitere Informationen finden Sie unter "Hinzufügen oder Entfernen eines Back-End-Servers" weiter unten in diesem Thema. Beachten Sie, dass dieses Verfahren nur für MAPI gilt.

Inhalt auf dem Back-End-Server nicht verfügbar

In der Front-End- und Back-End-Topologie wird ein besonderes Verfahren angewandt, wenn der Back-End-Server eine Anfrage für einen Öffentlichen Ordner erhält, für den er kein Replikat besitzt. Dieses Verfahren gilt neben Ordnern in den allgemeinen Öffentliche Ordner-Strukturen auch für Ordner im Standardinformationsspeicher für Öffentliche Ordner.

Wenn ein Back-End-Server eine solche Anfrage empfängt, gibt er eine Liste mit Servern zurück, die den Inhalt des angeforderten Ordners enthalten. Der Front-End-Server leitet diese Informationen nicht an den Client zurück, führt jedoch denselben Hashalgorithmus für die neue Serverliste erneut aus, um den Lastenausgleich und konsistente Ansichten sicherzustellen. In Organisationen mit Teilreplikaten von Öffentliche Ordner-Strukturen muss der Front-End-Server möglicherweise zwei HTTP-Anfragen verarbeiten, um eine einzelne Anfrage vom Client zu beantworten. Durch die Verarbeitung der Clientanfrage speichert der

Front-End-Server jedoch Informationen darüber, welche Server über den Inhalt verfügen. Front-End-Server können daher zusätzliche Anfragen vermeiden, wenn auf denselben Ordner zukünftig zugegriffen wird.

Die vom Front-End-Server verwalteten Caches vermindern die Anzahl der an Active Directory und Back-End-Server gesendet Anfragen sowohl für öffentliche als auch für private Ordnerzugriffe erheblich. Cacheinformationen laufen nach zehn Minuten ab und werden bei Änderungen in der Serverkonfiguration neu festgelegt.

Hinweis:

Exchange 5.5-Server können nicht ausgewählt werden, da sie die erforderlichen HTTP WebDAV-Erweiterungen nicht unterstützen.

Ausfallzeiten bei Back-End-Servern

Wenn ein Back-End-Server aufgrund von Wartungsmaßnahmen ausfällt oder der Zugriff über HTTP aus anderen Gründen nicht möglich ist, kann der Front-End-Server keine Verbindung zu ihm herstellen. Der Front-End-Server kennzeichnet den Server für einen Zeitraum von 10 Minuten als "nicht verfügbar" und sendet eine Anfrage an einen anderen Server, falls andere Server verfügbar sind. Die Anfrage schlägt fehl, wenn kein anderer Server vorhanden ist. Während der Back-End-Server nicht verfügbar ist, leitet der Front-End-Server die Anfragen automatisch an andere Server weiter. Wenn ein Back-End-Server wieder betriebsbereit ist, ist der Zugriff über den Front-End-Server möglicherweise für 10 Minuten blockiert, weil der Front-End-Server ihn unter Umständen immer noch als nicht verfügbar gekennzeichnet hat.

Dieser Prozess steigert die Zuverlässigkeit für den Zugriff auf Öffentliche Ordner erheblich. Der Front-End-Server kontaktiert mehrere Back-End-Server in Bezug auf die Daten, wohingegen ein Client mit einer direkten Verbindung zu einem Back-End-Server dies nicht tut.

Hinzufügen oder Entfernen von Back-End-Servern

Ziel des Hashalgorithmus ist der Lastenausgleich. Eine Bedingung dieses Algorithmus ist jedoch, dass die Verteilung von Benutzern auf die Server von der Anzahl der Server abhängt. Wenn der Liste der Server, die den Inhalt für einen Öffentlichen Ordner hostet, Server hinzugefügt oder daraus entfernt werden, wird der Benutzer durch den Hashalgorithmus möglicherweise an einen neuen Server für zukünftige Anfragen geleitet. Bis auf folgende Ausnahme kann der Benutzer während der Verarbeitung einer Anfrage durch den Server keine Mitteilung über eine physikalische Änderung erteilen:

- Benutzer können feststellen, ob der Status "Lesen" bzw. "Nicht gelesen" von Nachrichten zurückgesetzt wurde.
- Benutzer von webbasierten Anwendungen (die in allgemeinen Öffentlicher Ordner-Strukturen ausgeführt werden), die den Sitzungsstatus beibehalten, müssen ihre

Anwendungssitzung neu starten, wenn sie die Anwendung während der Übergansphase verwenden.

Es wird daher empfohlen, dass Administratoren ihre Benutzer vor dem Hinzufügen von Ordnerinhalt zu Öffentliche Ordner-Servern bzw. vor dem Entfernen von Inhalt informieren.

Auf hohem Niveau wird der Hashalgorithmus wie folgt ausgeführt: Zwei Back-End-Server mit den Nummern 1 und 2, auf denen der Inhalt eines Öffentlichen Ordners gespeichert ist. Wenn unterschiedliche Benutzer (A, B, C, D, E und F) versuchen, auf die Daten in diesem Ordner zuzugreifen, verteilt der Front-End-Server ihre Anfragen wie folgt über die beiden Server:

- Benutzer A, B und C erhalten ihre Daten von Server 1.
- Benutzer D, E und F erhalten ihre Daten von Server 2.

Hinweis:

Dieser Lastenausgleich ist transparent, Benutzer wissen nicht, welcher Back-End-Server die Anfrage aktuell verarbeitet.

Dann wird ein weitere Server (Server 3) hinzugefügt, und der Inhalt wird ebenfalls auf diesen Server repliziert. Die Benutzer werden anschließend wie folgt verteilt:

- Benutzer A und B erhalten die Daten von Server 1.
- Benutzer C un D erhalten die Daten von Server 2.
- Benutzer E und F erhalten die Daten von Server 3.

In diesem Beispiel haben Benutzer C, E und F die Server gewechselt, Benutzer A, B und D hingegen nicht.

Vereinfachen der Outlook Web Access-URL

Benutzer fordern häufig für den Zugriff auf ihr Postfach eine einfachere Outlook Web Access-URL. Bei diesem Verfahren wird eine an das Stammverzeichnis des Webservers (**http://server/**) gesendete Anforderung konfiguriert, um sie zum virtuellen Exchange-Verzeichnis umzuleiten. So wird beispielsweise eine Anforderung an **https://mail/** zu **https://mail/exchange/** umgeleitet und damit die implizite Anmeldung ausgelöst.

Bevor Sie beginnen

Bevor Sie das in diesem Thema beschriebene Verfahren durchführen, lesen Sie bitte den Abschnitt "Funktionsweise einer Front-End- und Back-End-Topologie" im Front-End- und Back-End-Topologie unter Exchange Server 2003 und Exchange 2000 Server-Handbuch.

Zum erfolgreichen Durchführen der Verfahren dieses Themas müssen folgende Voraussetzungen erfüllt sein:

- Die Authentifizierung für den Front-End-Server ist aktiviert.

Verfahren

So vereinfachen Sie die Outlook Web Access-URL

1. Öffnen Sie mit dem Internetdienste-Manager die Eigenschaften für die Standardwebsite.
2. Klicken Sie auf die Registerkarte **Basisverzeichnis**, und aktivieren Sie dann **auf einer Umleitung zu einem URL**.
3. Geben Sie /**<Verzeichnisname>** unter **Umleiten zu** ein, und klicken Sie anschließend auf **einem Verzeichnis unterhalb des angegebenen URL**. Um beispielsweise Anforderungen an **https://mail/** zu **https://mail/exchange** umzuleiten, geben Sie /**exchange** unter **Umleiten zu** ein.

Wenn Benutzer über SSL auf den Server zugreifen sollen, können Sie die Clientanforderungen zu **https://mail/<directory name>** umleiten. Zum Erzwingen der Verwendung von SSL geben Sie **https://mail/<Verzeichnisname>** unter **Umleiten zu** ein, und klicken Sie anschließend auf **einem Verzeichnis unterhalb des angegebenen URL**. Durch diese Einstellung wird der Name des Servers fest codiert. Wenn Sie Clientanforderungen zu **https://mail** umleiten, muss daher der Client den Namen **mail** auflösen können.

Hinweis:

Benutzer müssen dennoch die vollständige URL angeben, einschließlich des Benutzernamens, um auf andere Postfächer oder auf den Inhalt anderer Ordner außer dem Posteingang zuzugreifen.

Weitere Informationen

Weitere Informationen über das Aktivieren der Authentifizierung auf dem Front-End-Server (auch als "implizite Anmeldung" bezeichnet) finden Sie unter "Funktionsweise einer Front-End- und Back-End-Topologie" im Front-End- und Back-End-Topologie unter Exchange Server 2003 und Exchange 2000 Server-Handbuch.

Authentifizierungsmechanismen für HTTP

Der Front-End-Server führt die Authentifizierung wie folgt durch: entweder er authentifiziert den Benutzer selbst (mit Standard- oder formularbasierter Authentifizierung), oder er leitet die Anfrage anonym an den Back-End-Server weiter. Der Back-End-Server wendet ebenfalls eine dieser beiden Authentifizierungsarten an.

Hinweis:

Auf dem Front-End-Server ist eine anonyme Authentifizierung erforderlich, wenn er in einem Umgebungsnetzwerk positioniert ist und RPCs (Remote Procedure Calls, Remoteprozeduraufrufe) nicht verwenden kann. Die ist kein empfohlenes Szenario, da der Benutzerzugriff vom Front-End-Server nicht geblockt werden kann. Weitere Informationen zur Pass-Through-Authentifizierung finden Sie unter "Pass-Through-Authentifizierung" weiter unten in diesem Thema.

Wichtig:

Die Verwendung der dualen Authentifizierung wird dringend empfohlen. Bei dieser Authentifizierung werden sowohl Front-End- als auch Back-End-Server zur Authentifizierung von Benutzern konfiguriert. Weitere Informationen finden Sie im Abschnitt "Duale Authentifizierung" weiter unten in diesem Thema.

Duale Authentifizierung

Die duale Authentifizierung wird standardmäßig mit Front-End- und Back-End-Servern verwendet. Bei der dualen Authentifizierung werden sowohl die Front-End- als auch die Back-End-Server zur Authentifizierung von Benutzern konfiguriert. Konfigurieren Sie sofern möglich die Front-End-Server immer für die Authentifizierung. Wenn die Authentifizierung auf dem Front-End-Server nicht aktiviert werden kann, können sich Benutzer nicht implizit anmelden, und der Lastenausgleich von Anfragen für Öffentliche Ordner kann nicht realisiert werden. Die explizite Anmeldung ist unabhängig von der jeweils konfigurierten Authentifizierung möglich.

Hinweis:

Exchange benötigt IIS zur Authentifizierung von HTTP-Anfragen. IIS verwendet die RPC-Authentifizierung für Verzeichnisserver. Wenn RPCs zwischen dem Front-End-Server und dem Verzeichnisserver nicht erlaubt sind, müssen Sie die Pass-Through-Authentifizierung verwenden. Weitere Informationen zur Aktivierung der Pass-Through-Authentifizierung und den damit verbundenen Risiken finden Sie unter "Pass-Through-Authentifizierung" weiter unten in diesem Thema.

Pass-Trought-Authentifizierung

Bei der Pass-Through-Authentifizierung ist der Front-End-Server mit anonymer Authentifizierung konfiguriert und ruft daher keinen Autorisierungsheader beim Benutzer ab. Der Front-End-Server leitet die Anfrage des Benutzers an den Back-End-Server weiter, der den Benutzer zur Authentifizierung auffordert. Die Authentifizierungsanfrage des Back-End-Servers und die Antwort des Benutzers werden unverändert über den Front-End-Server gesendet.

Hinweis:

Bei der Pass-Through-Authentifizierung werden anonyme HTTP-Anfragen direkt an den Back-End-Server geleitet und authentifiziert. Die Pass-Through-Authentifizierung sollte nur in absolut dringenden Fällen verwendet werden. Die empfohlene Strategie ist die Platzierung einer erweiterten Firewall im Umgebungsnetzwerk mit dem Front-End-Server hinter der internen Firewall, so dass er uneingeschränkten RPC-Zugriff auf das interne Netzwerk hat. Wenn Sie den Front-End-Server im Umgebungsnetzwerk platzieren möchten, ist es möglicherweise sicherer, RPCs anstelle von anonymen Anfragen zur Kontaktierung von Back-End-Servern zu erlauben, da mit der Pass-Through-Authentifizierung gültige oder ungültige Anfragen aus beliebigen Quellen an Ihre Back-End-Server weitergeleitet werden können. Weitere Informationen finden Sie unter Szenarien für die Bereitstellung einer Front-End- und Back-End-Topologie.

Bei Verwendung der Pass-Through-Authentifizierung kann der Front-End-Server kein Lastenausgleich für Öffentliche Ordner-Anfragen durchführen, da er nicht über das Authentifizierungstoken zur Durchführung eines Hash-Algoritmus verfügt. Weiterhin können sich Benutzer nicht implizit anmelden. Benutzer müssen einen vollständigen URL mit ihrem Benutzernamen eingeben, um sich anzumelden.

Authentifizierungsmethoden

Für Ihre Front-End- und Back-End-Serverarchitektur stehen je nach verwendeter Exchange-Version verschiedene Authentifizierungsmethoden zur Verfügung. Zudem bietet die Authentifizierung zwischen dem Client und dem Front-End-Server im Gegensatz zur Authentifizierung zwischen Front-End- und Back-End-Servern verschiedene Optionen. In den folgenden Abschnitten werden die beiden Authentifizierungsmethoden näher erläutert.

Authentifizierung zwischen Client und Front-End-Server

Hinweis:

Front-End-Server bieten keine Unterstützung für die integrierte Windows-Authentifizierung (NTLM- und Kerberos-Authentifizierung) oder die HTTP 1.1 Digest-Authentifizierung.

Standardauthentifizierung

Bei der Standardauthentifizierung handelt es sich um einen einfachen durch die HTTP-Spezifikation festgelegten Authentifizierungsmechanismus, der den Benutzernamen und das Kennwort des Benutzers vor dem Senden an den Server schwach kodiert. Für einen optimalen Kennwortschutz in einer Front-End- und Back-End-Topologie sollten Sie die SSL-Verschlüsselung zwischen dem Client und dem Front-End-Server verwenden.

Hinweis:

Standardauthentifizierung wird von Exchange 2000 Server und Exchange Server 2003 unterstützt.

Die Standardauthentifizierung bietet keine Unterstützung für die Einzelanmeldung. Einzelanmeldung findet statt, wenn sich ein Benutzer an einem Computer unter Windows anmeldet, sich für die Domäne authentifiziert und anschließend auf alle Ressourcen und Anwendungen in der Domäne zugreifen kann, ohne seine Anmeldeinformationen erneut einzugeben. Microsoft Internet Explorer Versionen 4.0 und höher unterstützen die Einzelanmeldung für Webanwendungen, einschließlich Outlook Web Access, wenn auf dem Server, auf den zugegriffen wird, die integrierte Windows-Authentifizierung aktiviert ist. Da Front-End-Server für den Zugriff auf HTTP-Anwendungen keine Unterstützung für die integrierte Windows-Authentifizierung bieten, fordert der Front-End-Server immer zur Authentifizierung und zur erneuten Eingabe von Anmeldeinformationen auf, auch wenn diese bei der Anmeldung an Windows bereits eingegeben wurden. In einer Browsersitzung müssen Benutzer jedoch nur einmal ihre Anmeldeinformationen eingeben, da diese während der Sitzung gespeichert werden.

Wichtig:

Achten Sie bei Verwendung eines Kiosk darauf, dass das Zwischenspeichern von Anmeldeinformationen ein Sicherheitsrisiko darstellt, wenn Sie den Browser nicht schließen können und ihn zwischen Sitzungen schließen. Dieses Risiko tritt auf, da die Benutzeranmeldeinformationen im Cache verbleiben, wenn der nächste Benutzer auf den Kiosk zugreift. Stellen Sie zur Aktivierung von Outlook Web Access im Kioskmodus sicher, dass Sie den Browser zwischen Sitzungen schließen und den Browserprozess beenden können. Verwenden Sie andernfalls ein Drittanbieterprodukt mit Zweifaktor-Authentifizierung, bei der der Benutzer ein

physikalisches Token mit einem Kennwort zur Verwendung von Outlook Web Access im Kiosk angeben muss.

Formularbasierte Authentifizierung

Hinweis:

Die formularbasierte Authentifizierung wird nur in Exchange Server 2003 unterstützt. Sie können jedoch einen Front-End-Server unter Exchange Server 2003 mit einem Back-End-Server unter Exchange Server 2000 verwenden, um die Vorteile der formularbasierten Authentifizierung zu nutzen.

Die formularbasierte Authentifizierung verwendet ein Cookie, um den Benutzer nach der ersten Anmeldung zu identifizieren. Durch die Verfolgung dieser Cookie-Verwendung kann Exchange inaktive Sitzungen beenden. Vergleichbar mit der Standardauthentifizierung werden der anfänglich eingegebene Benutzername und das Kennwort jedoch nach wie vor in Klartext übertragen. Aus diesem Grund ist die Verwendung von SSL-Verschlüsselung mit formularbasierter Authentifizierung erforderlich. Weitere Informationen zur Konfiguration der formularbasierten Authentifizierung finden Sie im Abschnitt "Konfigurieren von formularbasierter Authentifizierung für Exchange Server 2003" in Konfigurieren eines Front-End-Servers als Standarddomäne.

Front-End/Back-End-Authentifizierung

Der Front-End-Server muss die Benutzerinformationen mit den Webanfragen an den Back-End-Server senden, damit der Back-End-Server Zugriff auf die Daten gewähren kann.

Integrierte Authentifizierung

Exchange 2003-Front-End-Server verwenden Kerberos-Authentifizierung zum Sichern von Benutzeranmeldeinformationen zwischen Front-End- und Back-End-Servern. Wenn die Kerberos-Authentifizierung fehlschlägt, wird ein Warnereignis protokolliert, und der Front-End-Server schaltet auf die Verwendung von NTLM um. Wenn NTLM fehlschlägt, wird ein Fehler protokolliert und auf die Standardauthentifizierung umgeschaltet.

Um dem Front-End-Server die Verwendung der integrierten Authentifizierung zu ermöglichen, ist die Konfiguration der integrierten Authentifizierung auf den virtuellen Back-End-Servern erforderlich (Standardkonfiguration).

Hinweis:

Sowohl Exchange 2003- als auch Exchange 2000-Back-End-Server unterstützen die integrierte Authentifizierung von einem Exchange 2003-Front-End-Servers.

Standardauthentifizierung

Der Front-End-Server leitet die Anmeldeinformationen der Standardauthentifizierung über Proxy an die Back-End-Server weiter. Zum Sichern dieser Informationen wird die Verwendung von IPSec zwischen den Front-End- und Back-End-Servern dringend empfohlen.

Hinweis:

Standardauthentifizierung zwischen den Front-End- und Back-End-Server wird von Exchange 2000- und Exchange 2003-Front-End-Servern unterstützt.

Benutzeranmeldeinformationen

Bei der Authentifizierung an einem Front-End-Server muss der Benutzer standardmäßig seinen Benutzernamen in folgendem Format eingeben: *domäne**benutzername*. Sie können einen Front-End-Server als Standarddomäne konfigurieren, damit sich Benutzer ihre Domäne nicht merken müssen.

Eine weitere Authentifizierungsoption ist die Konfiguration eines Benutzerprinzipalnamens (User Principal Name, UPN) für Benutzer. Normalerweise entspricht der Prinzipalname eines Benutzers seiner E-Mail-Adresse. Mit dieser Option können Benutzer ihre UPN/E-Mail-Adresse als ihren Benutzernamen eingeben. Weitere Informationen finden Sie unter Konfigurieren von Exchange-Front-End-Servern.

Remoteprozeduraufrufe (Remote Procedure Calls, RPCs) in der Exchange-Front-End- und Back-End-Topologie

DSAccess verwendet nicht mehr RPCs zur Ausführung der Active Directory-Diensterkennung. RPCs werden jedoch weiterhin für andere Aufgaben eingesetzt. Informationen zur Deaktivierung von RPCs finden Sie unter Konfigurieren von DSAccess für Perimeternetzwerke. IIS verwendet RPCs jedoch nach wie vor zur Authentifizierung von Anfragen auf dem Front-End-Server. Wenn Sie die Authentifizierung auf dem Front-End-Server aktivieren (was dringend empfohlen wird), muss dieser in der Lage sein, RPCs zu verwenden. Die Platzierung des Front-End-Servers hinter der internen Firewall wird für dieses Szenario empfohlen und sollte kein Problem darstellen. Wenn Sie Ihren Front-End-Server jedoch in einem Umkreisnetzwerk einsetzen, müssen Sie bestimmte RPC-Anschlüsse öffnen. Weitere Informationen zum Öffnen von RPC-Anschlüssen auf der internen Firewall finden Sie unter Konfigurieren einer Intranetfirewall.

Verlust von Features durch Platzierung eines Exchange-Front-End-Servers im Umkreisnetzwerk ohne RPC-Zugriff

Wichtig:

Die Informationen in diesem Abschnitt gelten für Benutzer, die einen Exchange-Front-End-Server in einem Umkreisnetzwerk platzieren und RPC-Datenverkehr über die interne Firewall nicht zulassen.

Unternehmen mit Umkreisnetzwerken beschränken häufig den Datenverkehr, der vom Umkreisnetzwerk in das Unternehmensintranet weitergeleitet wird.

Ohne RPC-Zugriff auf Active Directory-Server kann der Front-End-Server keine Clients authentifizieren. Features, die auf dem Front-End-Server authentifiziert werden müssen (wie zum Beispiel implizite Anmeldung und Lastenausgleich der Öffentliche Ordner-Struktur), können daher nicht ausgeführt werden. Der Zugriff auf Öffentliche Ordner ist möglich, der Front-End-Server kann jedoch keinen Lastenausgleich von Anfragen vornehmen, da er die Identität des Benutzers nicht bestimmen kann. Ohne Authentifizierungstoken des Benutzers kann der Front-End-Server den Hashalgorithmus für den Lastenausgleich nicht ausführen. Alle anonyme Anfragen für einen Öffentlichen Ordner werden daher an denselben Back-End-Server geleitet.

Hinweis:

Bei diesem Verfahren empfiehlt es sich, einen erweiterten Firewallserver (wie zum Beispiel ISA Server) anstelle des Front-End-Servers im Umkreisnetzwerk einzusetzen. Weitere Informationen finden Sie unter Erweiterte Firewall in einem Umgebungsnetzwerk.

Hinweis:

IMAP- und POP-Clients benötigen SMTP zum Senden von E-Mail-Nachrichten. Wenn Sie RPC-Datenverkehr über die interne Firewall nicht zulassen, können Sie SMTP auf dem Front-End-Server zur Unterstützung für IMAP- und POP-Clients nicht ausführen, da durch die Blockierung des RPC-Datenverkehrs MSExchangeIS auf dem Front-End-Server nicht ausgeführt werden kann. Sie können jedoch einen separaten Server zum Ausführen der SMTP-Funktionen für IMAP- und POP-Clients einrichten.

Wenn RPC-Anschlüsse zwischen dem Umkreisnetzwerk und dem Unternehmensintranet nicht erlaubt sind, müssen Sie die Pass-Through-Authentifizierung verwenden. Mit der Pass-Through-Authentifizierung leistet der Front-End-Server Anfragen an den Back-End-Server anonym weiter. Anschließend führt der Back-End-Server die Authentifizierung aus.

Überlegungen zur Bereitstellung einer Front-End- und Back-End-Topologie

Bei der Bereitstellung einer Front-End- und Back-End-Topologie müssen Sie einige Faktoren berücksichtigen, zum Beispiel die erwartete Netzwerklast, Hardwareanforderungen, Verwaltungsaufwand, Lastenausgleich und Sicherheit. In den folgenden Abschnitten werden diese Faktoren im Detail erläutert.

Keine Clusterbildung bei Front-End-Servern

Die Clusterbildung der Exchange-Front-End-Server bietet keine Verbesserung der Leistung. Front-End-Server haben keinen Status, so dass die Leistung viel höher ist, wenn zwei separate Server Verbindungen gemeinsam verwenden (oder Netzwerklastenausgleich betreiben). Die Clusterbildung ist daher nicht erforderlich.

Empfohlene Serverkonfigurationen und Einschätzungen

Serverkonfigurationen hängen von vielen Faktoren ab, wie zum Beispiel von der Anzahl der Benutzer für jeden Back-End-Server, den verwendeten Protokollen und der erwarteten Systemlast. Die Konfiguration bestimmter Servermodelle sollte mit einem Hardwareanbieter oder -berater durchgeführt werden.

In der Regel sollte ein Front-End-Server für vier Back-End-Server eingesetzt werden. Diese Anzahl ist jedoch nur ein Vorschlag bzw. ein Ausgangspunkt und sollte nicht als Regel betrachtet werden. Front-End-Server benötigen keinen großen bzw. besonders schnellen Plattenspeicher. Sie sollten jedoch schnelle CPUs und einen großen Arbeitsspeicher besitzen. Die Festplatten auf dem Front-End-Server müssen nur bei SMTP-Aktivierung gesichert werden, da SMTP der lokalen Festplatte E-Mail-Nachrichten aus der Warteschlange übergibt. Für POP, IMAP und HTTP werden keine Benutzerdaten auf dem Laufwerk gespeichert.

Weitere Informationen zu Hardwareanforderungen für Front-End- und Back-End-Server finden Sie in den folgenden technischen Dokumentationen:

- Exchange 2000 Front-End Server and SMTP Gateway Hardware Scalability Guide
- Exchange 2000 Server Back-End Mailbox Scalability

Lastenausgleich

In einer Unternehmens- oder Hostingumgebung empfiehlt sich unter Umständen der Lastenausgleich der Front-End-Server. Unter Windows steht diese Funktion über NLB (Network Load Balancing, Netzwerklastenausgleich) zur Verfügung. Alternativ dazu können andere Lastenausgleichs-Mechanismen verwendet werden, einschließlich Hardwarelösungen.

Beim Netzwerklastenausgleich unter Windows werden zwei oder mehrere Server in einem Cluster verbunden, der den NLB-Cluster mit einer einzelnen IP-Adresse bildet. Jeder Computer empfängt den Datenverkehr an seine eigene eindeutige IP-Adresse und an die gemeinsame IP-Adresse. Alles Mitglieder des NLB-Clusters führen einen Hashing-Algorithmus aus, um eingehende Clients einem Element des NLB-Clusters basierend auf der IP-Adresse, dem Anschluss und weiteren Clientinformationen zuzuordnen. Beim Eintreffen eines Datenpakets führen alle Server oder Hosts denselben Hashalgorithmus durch. Als Ergebnis wird einer der Hosts ermittelt. Dieser Host antwortet dann auf das Datenpaket. Die Zuordnung ändert sich nur, wenn sich die Anzahl der Hosts im NLB-Cluster ändert. Die Konfiguration der einzelnen Server im NLB-Cluster muss identisch sein. Andernfalls reagieren die Server unterschiedlich auf Clientanfragen.

Hinweis:

NLB verfügt nicht über die Zustandsüberwachungsfunktion. Wird der WWW-Publishingdienst auf einem Front-End-Server zum Beispiel nicht ausgeführt, sendet NLB weiterhin Anfragen an diesen Server. Sie können Microsoft Application Center 2000 auf einem Front-End-Server zum Einrichten von NLB sowie zum Überwachen des Zustands auf Servern mit aktiviertem Lastenausgleich ausführen. (Sie können Exchange-Ressourcen jedoch nicht verwalten oder Exchange-Konfigurationsinformationen über Application Center replizieren.) Weitere Informationen zu Application Center finden Sie auf der Website Microsoft Application Center.

Auch wenn es nicht erforderlich ist, sollten Sie sicherstellen, dass alle Benutzer für die Dauer einer Sitzung an denselben Front-End-Server gesendet werden. Hierfür werden SSL (Secure Sockets Layer)-Handshake-Informationen zum Zwischenspeicher und Verbindungsstatus verwendet, die bereits vom Server verwaltet werden. Weiterhin ist dies für die formularbasierte Authentifizierung erforderlich, da nur der Front-End-Server, der den Cookie herausgibt, diesen entschlüsseln kann. In NLB wird dies als "Clientaffinität" bezeichnet. Viele Hardwarelösungen weisen diese Fähigkeit auf.

Hinweis:

Erweiterte Firewallserver beeinträchtigen möglicherweise die NLB-Clusterbildung Ihrer Front-End-Server, besonders wenn sie die eingehende IP-Adresse verschleiern. Weitere Informationen finden Sie in der Produktdokumentation oder bei Ihrem Hersteller.

Reduzieren der virtuellen Servererstellung

In einigen Situationen kann es wichtig sein, die Anzahl der auf den Back-End-Servern erstellten virtuellen Servern zu reduzieren. Sie sollten die Anzahl der virtuellen Server nur dann reduzieren, wenn Sie umfassende Kenntnisse über die Funktionsweise von virtuellen HTTP-Servern besitzen. Das Erstellen von virtuellen Servern kann anhand von zwei Methoden reduziert werden.

Analysieren Sie die Benutzer und Daten auf allen Back-End-Servern, um zu ermitteln, ob Benutzer überhaupt zu diesem speziellen Server geleitet werden. Wenn ein Back-End-Server nur Postfächer für adatum.com enthält, muss dieser Back-End-Server nicht über einen virtuellen Server für contoso.com verfügen. Wenn Benutzer von contoso.com diesem Back-End-Server anschließend jedoch hinzugefügt, muss ein Administrator einen virtuellen Server für contoso.com erstellen.

Das Erstellen von virtuellen Verzeichnissen für Ressourcen ist nur erforderlich, wenn Benutzer auf diese zugreifen müssen. Auf einem Server ohne Informationsspeicher für Öffentliche Ordner ist ein öffentlicher virtueller Speicher nicht erforderlich.

Verwenden von Firewalls in einer Front-End- und Back-End-Topologie

Wenn Ihr Netzwerk über das Internet angezeigt werden kann, sollten Sie unbedingt eine software- oder hardwarebasierte Firewalllösung einsetzen. Firewalls steuern den Datenverkehr zum Netzwerk mit Methoden wie Anschlussfilterung, IP-Filterung und Anwendungsfilterung in erweiterten Firewalllösungen.

Zur Einbindung einer Firewall in eine Front-End- und Back-End-Topologie stehen mehrere Optionen zur Verfügung, die unter Szenarien für die Bereitstellung einer Front-End- und Back-End-Topologie. Grundsätzlich wird die Verwendung eines erweiterten Firewallservers in Ihrer Topologie empfohlen (weitere Informationen zur Verwendung einer erweiterten Firewall finden Sie unter Erweiterte Firewall in einem Umgebungsnetzwerk).

Anschlussfilterung

Die von Ihnen eingesetzte Firewall zum Schutz Ihrer Server vor dem Internet muss mindestens über die Anschlussfilterungsfunktion verfügen. Mit der Anschlussfilterung wird der über die Firewall eingehende Netzwerkdatenverkehr beschränkt, indem der Zugriff auf Informationen lediglich über bestimmte Anschlüsse gewährt wird. Sie können zum Beispiel die Firewall so konfigurieren, dass lediglich HTTPS-Datenverkehr über den TCP/IP-Anschluss 443 aus dem Internet akzeptiert wird.

In den folgenden beiden Abschnitten werden zwei wichtige Konzepte im Zusammenhang mit TCP/IP-Verbindungen erläutert: Quellanschluss im Vergleich zu Zielanschluss sowie die Richtung der TCP/IP-Verbindung.

Quellanschluss im Vergleich zu Zielanschluss

Wenn Computer A eine TCP/IP-Verbindung zu Computer B herstellt, werden zwei Anschlüsse verwendet: Der Quellanschluss (auf Computer A) und der Zielanschluss (auf Computer B). Der Netzwerkstack auf dem Computer, der die Verbindung initiiert, wählt die Quellanschlüsse normalerweise zufällig aus. Bei Zielanschlüssen handelt es sich um Anschlüsse, die der angegebene Dienst abhört (z. B. Anschluss 443 für HTTPS). Alle in diesem Handbuch enthaltenen Verweise auf einen von einem bestimmten Dienst verwendeten Anschluss beziehen sich auf den Zielanschluss.

Richtung der TCP-Verbindung

Beim Öffnen von Firewallanschlüssen müssen Sie bei den meisten Firewalls die Richtung der Verbindung angeben. Um beispielsweise den Kontakt von einem Front-End-Server zu Back-End-Servern herzustellen, müssen Sie Anschluss 80 für HTTP-Datenverkehr öffnen. Back-End-Server initiieren hingegen nie TCP/IP-Verbindungen zum Front-End-Server. Die antworten nur auf Anfragen, die vom Front-End-Server initiiert wurden. Auf Ihrer Firewall müssen Sie daher lediglich Anschluss 80 für HTTP-Verbindungen vom Front-End zum Back-End aktivieren. In diesem Handbuch werden solche Verbindung als "eingehend" bezeichnet (die Verbindungen werden von "außen" zum Unternehmensnetzwerk hergestellt).

IP-Filterung

Viele Firewalllösungen bieten ebenfalls Unterstützung für IP-Filterung. IP-Filterung steigert die Verlässlichkeit einer Firewall, da der Datenverkehr über die Firewall auf bestimmte Server beschränkt werden kann. In einem Umgebungsnetzwerk möchten Sie beispielsweise DSAccess zur Verwendung von bestimmten Domänencontrollern und globalen Katalogservern konfigurieren und anschließend IP-Filter einsetzen, um sicherzustellen, dass die Front-End-Server nur Verbindungen zu diesen Domänencontrollern und globalen Katalogservern herstellen.

Anwendungsfilterung

Erweiterte Firewalls wie z. B. ISA Server bieten eine erweiterte Überwachung auf der Anwendungsprotokollebene. Anhand dieser Überwachung kann die Firewall bestimmte Funktionen ausführen, wie zum Beispiel das Filtern von RPC-Schnittstellen und die Validierung der HTTP-Anfragesyntax. Anwendungsfilterung ist das Hauptargument für den Einsatz einer erweiterten Firewall in Ihrer Topologie. Sie bietet ein Höchstmaß an Sicherheit.

Unterstützung für sichere Kommunikation zwischen Client und Front-End Server

Zur Gewährleistung einer sicheren Datenübertragung zwischen dem Client und dem Front-End-Server wird dringend empfohlen, dass der Front-End-Server SSL-fähig ist. Für einen umfassenden Schutz der Benutzerdaten sollte der Zugriff auf den Front-End-Server ohne SSL deaktiviert werden (dies ist eine Option bei der SSL-Konfiguration). Bei Verwendung der Standardauthentifizierung sollte der Netzwerkverkehr unbedingt durch SSL gesichert werden, um Benutzerkennwörter vor nicht autorisierter Einsichtnahme in Netzwerkpakete zu schützen.

Hinweis:

Wenn Sie zwischen Clients und dem Front-End-Server kein SSL verwenden, ist die Datenübertragung zum Front-End-Server nicht sicher. Es wird dringend empfohlen, den Front-End-Server so einzurichten, dass SSL erforderlich ist.

Sie sollten nach Möglichkeit ein SSL-Zertifikat von einer Zertifizierungsstelle eines Drittanbieters erwerben. Der Erwerb eines Zertifikats von einer Zertifizierungsstelle ist die bevorzugte Methode, da die meisten Browser viele dieser Zertifizierungsstellen als vertrauenswürdig anerkennen.

Verwenden Sie Microsoft Certificate Server, um Ihre eigenen Zertifizierungsstellen zu installieren. Diese Methode ist zwar unter Umständen kostengünstiger, hat jedoch den Nachteil, dass Browser die Zertifikate nicht als vertrauenswürdig anerkennen und eine entsprechende Warnmeldung angezeigt wird.

Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 320291, "XCCC: Aktivieren von SSL für Exchange 2000 Server Outlook Web Access."

Konfigurieren von SSL in einer Front-End- und Back-End-Topologie

Wenn Sie einen Front-End-Server einsetzen, ist die Konfiguration von SSL auf den Back-End-Servern nicht erforderlich, da der Front-End-Server die Verwendung von SSL zur Kommunikation mit Back-End-Servern nicht unterstützt. Sie können SSL auf Back-End-Servern für Clients konfigurieren, die direkt auf diese zugreifen.

Wenn HTTP für den Datenzugriff verwendet wird, müssen Back-End-Server absolute URLs generieren, wie zum Beispiel eine Liste mit URLs für Nachrichten im Posteingang eines Benutzers. Wenn SSL zwischen dem Client und dem Front-End-Server verwendet wird, muss der Back-End-Server darüber informiert werden, um URLs mit HTTPS anstelle von HTTP zu formulieren. Wenn die SSL-Verschiebung auf dem Front-End-Server abgeschlossen ist, weiß der Front-End-Server, dass SSL verwendet wurde und

benachrichtigt den Back-End-Server über einen "Front-End-Https: on"-HTTP-Header, indem er einen HTTP-Header mit dem Hinweis "Front-End-Https: on" in allen Anfragen an den Back-End-Server weiterleitet.

Wenn ein separater Server zwischen dem Client und dem Front-End-Server die SSL-Entschlüsselung verschiebt, weiß der Front-End-Server nicht, dass die ursprüngliche Anfrage unter Verwendung von SSL durchgeführt wurde. In diesem Fall muss der Server in der Lage sein, den "Front-End-Https: on"-Header an den Front-Server zu übergeben, der diesen anschließend an den Back-End-Server zurückgibt. ISA Server bietet dafür Unterstützung. Informationen zu dieser Aktivierung finden Sie im Microsoft Knowledge Base-Artikel 307347, "Sichere OWA-Veröffentlichung hinter ISA Server kann benutzerdefinierten HTTP-Header erfordern."

Alternativ dazu können Sie SSL zwischen dem SSL-Entschlüsselungsserver und dem Front-End-Server konfigurieren. Wenn Sie jedoch einen separaten Server zum Verschieben von zusätzlichem durch SSL-Verschlüsselung und -Entschlüsselung entstandenen Datenverkehr hinzugefügt haben, ist diese Methode nicht geeignet. Bei dieser Methode kann der separate Server weiterhin den Datenverkehr filtern.

SSL-Beschleuniger

Da beim Einrichten von SSL-Verbindungen die Systemleistung abnimmt, können Sie Ihrer Front-End- und Back-End-Topologie einen SSL-Beschleuniger hinzufügen.

Es gibt zwei Arten von SSL-Beschleunigern:

- SSL-Beschleuniger-Netzwerkkarte, die Sie auf jedem Front-End-Server platzieren können.
- Einzelnes Gerät oder Computer, den Sie zwischen den Clients oder den Front-End-Servern platzieren können. Ein Beispiel für diese Beschleuniger ist das Microsoft Internet Security and Acceleration Server 2000 Feature Pack 1 Service Pack 1 (ISA). Diese Art von Beschleuniger unterstützt das Hinzufügen des "Front-End-Https: On"-Headers für Outlook Web Access.

Hinweis:

Informationen zum Konfigurieren des ISA-Servers für Outlook Web Access finden Sie im Microsoft Knowledge Base-Artikel 307347, "Sichere OWA-Veröffentlichung hinter ISA Server kann benutzerdefinierten HTTP-Header erfordern."

Beschleunigerkarten werden normalerweise direkt auf dem Front-End-Server verwendet und verschiebenden den aufgrund der Ver- und Entschlüsselung entstehenden Datenverkehr. Dadurch wird der Durchsatz jeder einzelnen Verbindung erhöht und die Software auf dem Server entlastet.

Externe Beschleunigergeräte sind zwischen den Clients und den Front-End-Servern positioniert. Der vom Client kommende Datenverkehr wird auf dem Beschleunigergerät

entschlüsselt und unverschlüsselt an den Front-End-Server weitergeleitet. Entsprechend wird der Datenverkehr vom Front-End-Server unverschlüsselt an das Beschleunigergerät und dann verschlüsselt an den Client weitergeleitet.

Der wichtigste Aspekt, den Sie bei der Auswahl des SSL-Beschleunigertyps beachten sollten, ist die Anzahl der Front-End-Server in Ihrer Topologie. Wenn Sie wenige Front-End-Server einsetzen, stellt das Hinzufügen von SSL-Beschleunigerkarten eine einfache und kostengünstige Möglichkeit dar, SSL-Aufgaben zu verschieben. Da die SSL-Entschlüsselung auf dem Front-End-Server stattfindet, ist die gesonderte Konfiguration des "Front-End-Https: on"-Headers für Outlook Web Access nicht erforderlich.

Bei einer großen Anzahl von Front-End-Servern sind die Kosten für zusätzliche Beschleunigerkarten und die Verwaltungskosten für das Speichern und Konfigurieren von SSL-Zertifikaten auf allen Servern möglicherweise zu hoch. In diesem Fall stellt ein separates SSL-Beschleunigergerät eine kostengünstigere Option für Ihre Topologie dar, da unabhängig von der Anzahl der Front-End-Server lediglich eine einmalige Konfiguration erforderlich ist. Diese Geräte kosten normalerweise mehr als eine Beschleunigerkarte. Wägen Sie daher die verschiedenen Optionen für Ihre Topologie ab. Beachten Sie, dass es für Outlook Web Access erforderlich ist, dass ein externes SSL-Gerät den Front-End-Server über die Verwendung von SSL mit dem "Front-End-Https: on"-Header informieren muss.

SSL-Verschiebung

Wenn ein separater Server zwischen dem Client und dem Front-End-Server die SSL-Verschlüsselung verschiebt, weiß der Front-End-Server nicht, dass die ursprüngliche Anfrage unter Verwendung von SSL durchgeführt wurde. In diesem Fall muss der Server in der Lage sein, den "Front-End-Https: on"-Header an den Front-Server zu übergeben, der diesen anschließend an den Back-End-Server zurückgibt.

Wenn Ihr Server für die SSL-Verschiebung das Hinzufügen eines benutzerdefinierten Headers nicht unterstützt, können Sie eine ISAP (Internet Server Application Programming Interface) auf dem Front-End-Server installieren, um diesen Header hinzuzufügen. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 327800, "How to configure SSL Offloading for Outlook Web Access in Exchange 2000 Server and in Exchange Server 2003". Alternativ dazu können Sie SSL zwischen dem SSL-Entschlüsselungsserver und dem Front-End-Server konfigurieren. Wenn Sie jedoch einen separaten Server zum Verschieben von zusätzlichem durch SSL-Verschlüsselung und -Entschlüsselung entstandenen Datenverkehr hinzugefügt haben, ist diese Methode ungeeignet. Bei dieser Methode kann der separate Server weiterhin den Datenverkehr filtern.

In diesem Fall stellt ein separates SSL-Beschleunigergerät eine kostengünstigere Option für Ihre Topologie dar, da unabhängig von der Anzahl der Front-End-Server lediglich eine einmalige Konfiguration erforderlich ist. Diese Geräte kosten normalerweise mehr als eine Beschleunigerkarte. Wägen Sie daher die verschiedenen Optionen für Ihre Topologie ab. Beachten Sie, dass es für Outlook Web Access erforderlich ist, dass ein externes SSL-Gerät

den Front-End-Server über die Verwendung von SSL mit dem "Front-End-Https: on"-Header informieren muss.

Formularbasierte Authentifizierung

Wenn Sie die formularbasierte Authentifizierung mit SSL-Verschiebung verwenden, müssen Sie Ihre Exchange-Front-End-Server für dieses Szenario konfigurieren. Ausführliche Anweisungen finden Sie unter Aktivieren der formularbasierten Authentifizierung bei Verwendung von SSL-Verschiebung.

Aktivieren der formularbasierten Authentifizierung bei Verwendung von SSL-Verschiebung

Wenn Sie die formularbasierte Authentifizierung mit verschobenem SSL (Secure Sockets Layer) verwenden, müssen Sie die Exchange Server-Front-End-Server für die Verarbeitung dieses Szenarios konfigurieren.

Bevor Sie beginnen

Dieses Thema enthält Informationen zum Bearbeiten der Registrierung.

Vorsicht:

Die fehlerhafte Bearbeitung der Registrierung kann zu ernsthaften Problemen führen, die möglicherweise eine Neuinstallation des Betriebssystems erforderlich machen. Dadurch entstandene Probleme können unter Umständen nicht mehr behoben werden. Sichern Sie vor dem Ändern der Registrierung alle wichtigen Daten.

Verfahren

So aktivieren Sie die formularbasierte Authentifizierung mit SSL-Verschiebung

1. Starten Sie den Registrierungs–Editor.
2. Suchen Sie den folgenden Registrierungsschlüssel: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWeb\OWA
3. Zeigen Sie im Menü **Bearbeiten** auf **Neu**, und klicken Sie dann auf **DWORD-Wert**.
4. Geben Sie im Detailausschnitt für den neuen Wert den Namen **SSLOffloaded** ein.

5. Klicken Sie auf den DWORD-Wert **SSLOffloaded** und dann auf **Ändern**.
6. Klicken Sie in **DWORD-Wert bearbeiten** unter **Basis** auf **Dezimal**.
7. Geben Sie im Feld **Wert** den Wert **1** ein.
8. Klicken Sie auf **OK**.

Hinweis:
Starten Sie den W3SVC-Dienst neu, um die Änderungen zu übernehmen.

Weitere Informationen

- Sie finden weitere Informationen über folgende Themen:
  - Überlegungen zur Bereitstellung einer Front-End- und Back-End-Topologie
  - "Aktivieren der formularbasierten Authentifizierung" im Handbuch für den Clientzugriff in Exchange Server 2003.

Sichern der Kommunikation von Front-End-Servern zu anderen Servern

Bei Verwendung von HTTP, POP und IMAP wird die Datenübertragung zwischen dem Front-End-Server und einem beliebigen anderen Server, mit dem der Front-End-Server kommuniziert (beispielsweise Back-End-Server, Domänencontroller und globale Katalogserver), nicht verschlüsselt. Wenn der Front-End- und Back-End-Server sich in einem vertrauenswürdigen physischen oder vermittelten Netzwerk befinden, ist diese Sicherung nicht von Bedeutung. Wenn Sie sich aber in separaten Subnets befinden, erfolgt der Netzwerkverkehr unter Umständen über unsichere Netzwerkbereiche. Das Sicherheitsrisiko nimmt zu, wenn zwischen dem Front-End- und Back-End-Server eine größere physische Distanz besteht. In diesem Fall ist es empfehlenswert, den Netzwerkverkehr zu verschlüsseln, um Kennwörter und Daten zu schützen.

IP Security (IPSec)

Windows unterstützt IPSec, ein Internetstandard zur Verschlüsselung von IP-Datenverkehr mit Ausnahme von Datenverkehr, der Broadcast- oder Multicast-IP-Adressen verwendet. Im Allgemeinen wird IPSec zur Verschlüsselung von HTTP-Verkehr verwendet. Sie können jedoch auch IPSec zur Verschlüsselung des Datenverkehrs einsetzen.

IPSec ermöglicht Folgendes:

- Konfigurieren von zwei Servern unter Windows für den vertrauenswürdigen Netzwerkzugriff.
- Übertragen von Daten, die schreibgeschützt sind (mithilfe einer kryptografischen Prüfsumme auf jedem Paket).
- Verschlüsseln von Datenübertragungen zwischen beiden Servern auf der IP-Ebene.

In einer Front-End-/Back-End-Topologie können Sie mithilfe von IPSec den Datenverkehr zwischen dem Front-End- und Back-End-Server verschlüsseln, der ansonsten nicht verschlüsselt würde.

IPSec-Protokolle

Die Methode zum Sichern von Daten mit IPSec richtet sich nach dem jeweils verwendeten Protokoll: AH (Authentication Header) oder ESP (Encapsulating Security Payload). Mit AH werden die Pakete nicht verschlüsselt. AH fügt dem IP-Paket eine Prüfsumme hinzu. AH garantiert, dass das vom erwarteten Host eingegangene Paket keine andere Identität angenommen hat und bei der Übertragung nicht geändert wurde. AH verwendet IP-Protokoll 51. ESP verwendet IP-Protokoll 50 und verschlüsselt den gesamten Inhalt des IP-Pakets. Beide Formen von IPSec bieten einen verlässlichen und vertrauenswürdigen Kommunikationskanal, in den ein Angreifer problemlos Daten einschleusen oder Unterbrechungen verursachen kann.

IPSec-Verschlüsselung wirkt sich auf die Leistung auf den Front-End- und Back-End-Servern aus. Die Auswirkungen im Einzelnen richten sich jedoch nach dem verwendeten Verschlüsselungstyp.

IPSec-Richtlinie

Sie sollten IPSec auf den Back-End-Servern konfigurieren, so dass diese beim Eingang einer Anfrage für IPSec-Kommunikation entsprechend antworten. Für die Back-End-Server ist es jedoch nicht erforderlich, dass die gesamte Kommunikation von allen Clients mit IPSec verschlüsselt wird.

In Windows werden standardmäßig drei IPSec-Richtlinien installiert. Wählen Sie die Richtlinie "Client (nur antworten)" für den Back-End-Server aus. Bei Aktivierung dieser Richtlinie auf dem Back-End-Server kann der Front-End-Server IPSec zur sicheren Kommunikation mit dem Back-End-Server verwenden, während andere Clients (einschließlich frühere Versionen von MAPI-Clients wie Microsoft® Office Outlook® 2002) und Server mit dem Back-End-Server kommunizieren können, ohne IPSec einsetzen zu müssen.

IPSec mit Firewalls und Filterrouter

Beim Einsatz einer Firewall und Filterrouter zwischen den Front-End- und Back-End-Servern müssen die Filter die Übermittlung von IPSec zulassen.

Hinweis:

IPSec funktioniert nicht, wenn sich zwischen dem Umkreisnetzwerk und dem Unternehmensnetzwerk ein NAT (Network Address Translation)-Server befindet.

Konfigurieren Sie die Anschlüsse beim Einsatz von IPSec wie folgt:

- **HTTP (TCP-Anschluss 80)** HTTP (TCP-Anschluss 80) wird nicht mehr benötigt und sollte gesperrt werden.
- **Andere Protokollanschlüsse** Wenn Sie IPSec zum Verschlüsseln des gesamten Datenverkehrs verwenden, benötigen Sie keine weiteren Protokollanschlüsse (außer ggf. Kerberos).
- **500/UDP** Öffnen Sie den IPSec-Anschluss an 500/UDP, der zur Kommunikation erforderlich ist. 500/UDP ist der bekannte, über das Internet zugewiesene Anschluss für den IKE (Internet Key Exchange)-Standard, der in RFC 2409 festgelegt ist. Dieser Standard verwendet UDP anstelle von TCP/IP, um die Sicherheitsschwachstellen bei TCP/IP-Verbindungen zu vermeiden. IKE bietet starke Sicherheit für den Austausch von Datenpaketen. IKE stellt IPSec-Verbindungen her und behält diese unter benannten Sicherheitszuweisungen bei.
- **IP-Protokoll 50 oder 51** Lassen Sie entweder IP-Protokoll 50 (AH) oder IP-Protokoll 51 (ESP) je nach verwendetem Protokoll zu.
- **UDP-Anschluss 88 und TCP-Anschluss 88** Kerberos wickelt den Datenverkehr über das UDP/TCP-Protokoll mit der Ausgangs- und Zieladresse 88 ab. Da Kerberos selbst ein Sicherheitsprotokoll ist, ist es nicht in den IPS-Filtern in Microsoft® Windows 2000 Server enthalten, obwohl die IPSec-Anschlüsse gefiltert werden. Bei Verwendung von IPSec unter Windows 2000 Server müssen UDP-Anschluss 88 und TCP-Anschluss 88 daher geöffnet sein. Alternativ dazu können Sie erzwingen, dass Kerberos in ein IPSec-Filter einbezogen wird, indem Sie den Registrierungsschlüssel "NoDefaultExempt" festlegen. In Windows Server 2003 wird Kerberos von IPSec-Filtern standardmäßig integriert. Wenn Kerberos in die IPSec-Verschlüsselung einbezogen wird, können Sie Kerberos nicht zur Authentifizierung der IPSec-Sitzung selbst verwenden. Verwenden Sie hierfür ein Zertifikat oder einen zuvor freigegebenen Schlüssel.
- Weitere Informationen zum Konfigurieren von IPSec mit Firewalls finden Sie im Microsoft Knowledge Base-Artikel 233256 mit Informationen zum Aktivieren von IPSec-Datenverkehr.
- Weitere Informationen zu IPSec und Kerberos finden Sie im Microsoft Knowledge Base-Artikel 810207 mit Informationen zum "Löschen von IPSec-Standardausnahmen in Windows Server 2003."

- In einem Umkreisnetzwerk möchten Sie die Sicherheit von IPSec möglicherweise erhöhen, ohne die Fähigkeit zu verlieren, den Datenverkehr aus Sicherheitsgründen zu filtern. In diesem Fall können Sie einen IPSec-Tunnel vom Front-End-Server zur internen Firewall und dann einen separaten Tunnel von der internen Firewall zum Back-End-Server einrichten. Dieses Verfahren sichert die Übertragungsinformationen und ermöglicht gleichzeitig den Einsatz von Filter- oder Angriffserkennungssoftware bzw. Techniken, bevor der Datenverkehr das interne Netzwerk erreicht.

Hinweis:

IPSec-Verschlüsselung findet statt, nachdem die Anwendung (in diesem Fall Exchange) die Anfrage an Windows zur Weiterleitung an den Server sendet. Die Anfrage wird, soweit Exchange betroffen ist, unter Verwendung von TCP/IP-Anschluss 80 über HTTP gesendet. Bevor jedoch die Daten den Server verlassen, werden sie abgefangen und möglicherweise verschlüsselt (wenn ESP konfiguriert ist) und dann über einen separaten Kanal gesendet (IP-Protokolle 50 oder 51). Die Verschlüsselung ist daher für die auf den Servern ausgeführten Exchange-Anwendungen nachvollziehbar und die Tatsache, dass die Daten nie Anschluss 80 in Anspruch nehmen, stellt keine Problem für diese Anwendungen dar.

Service Packs: Aktualisieren von Front-End- und Back-End-Servern

Dank der Veröffentlichung von neuen Service Packs stellt die Aktualisierung von Front-End-Servern ein recht einfaches Verfahren dar. Die Aktualisierung ist im Vergleich zu Back-End-Servern leichter, da auf dem Front-End-Server keine Benutzerdaten gespeichert werden. Wird beim Einsatz mehrerer Front-End-Server einer dieser Server offline geschaltet, führt dies zu keiner Unterbrechung für den Benutzer. Beim Lastenausgleich mehrerer Front-End-Server können Sie den Front-End-Server entfernen, den Sie aus dem Lastenausgleichscluster aktualisieren möchten, diesen anschließend aktualisieren und ohne Unterbrechung für den Benutzer dem Lastenausgleichscluster erneut hinzufügen.

Überlegungen zur Aktualisierung von Outlook Web Access

Wenn Outlook Web Access in Ihrer Organisation eingesetzt wird, sollten Sie vor der Aktualisierung von Back-End-Servern zunächst alle Front-End-Server aktualisieren. Dieses Verfahren ist aufgrund der Konzeption von Outlook Web Access erforderlich. Outlook Web Access besteht aus zwei Teilen auf hohem Leistungsniveau: Vorlagen und Steuerelemente. Vorlagen sind mit Formularen vergleichbar (E-Mail-Nachrichten, Kalenderobjekte und andere Formulare). Steuerelemente sind Dateien, wie zum Beispiel DHTML-Festlegungen, JScript®-

Dateien, Stylesheets und Bilder, die im virtuellen /exchweb-Verzeichnis von IIS gespeichert sind.

Wenn ein Benutzer über den Front-End-Server auf Outlook Web Access zugreift, werden die Vorlagen vom Back-End-Server und die Steuerelemente vom Front-End-Server bereitgestellt. Die Vorlagen werden aus Gründen der Leistungsfähigkeit vom Back-End-Server abgerufen. Die Steuerelemente stammen vom Front-End-Server, da eine Zwischenspeicherung von Anfragen vom Front-End-Server zum Back-End-Server nicht erfolgt, es sei denn, dass sie sich im Exchange-Informationsspeicher befinden. Dies stellt kein Problem dar, solange auf den Front-End- und Back-End-Servern dieselbe Version und dasselbe Service Pack von Exchange ausgeführt wird.

Ein Problem entsteht dann, wenn auf den Servern verschiedene Service Pack-Versionen ausgeführt werden. Wenn eine Vorlage auf einem Back-End-Server auf ein Steuerelement auf einem Front-End-Server verweist und auf dem Front-End-Server eine frühere Service Pack-Version ausgeführt wird, ist das Steuerelement, auf das der Back-End-Server verweist, möglicherweise nicht vorhanden. Outlook Web Access kann daher nicht von Benutzern eingesetzt werden, deren Postfächer sich auf dem aktualisierten Back-End-Server befinden.

Umgekehrt taucht dieses Problem nicht auf. Wenn Sie einen Front-End-Server zuerst aktualisieren, werden den Benutzern die Vorlagen des Back-End-Servers angezeigt. Diese Vorlagen verweisen auf die früheren auf dem Front-End-Server nach wie vor vorhandenen Steuerelementversionen, da den Dateien bei einer Aktualisierung lediglich eine andere Version zugewiesen, sie aber nicht gelöscht wurden. Zur Behebung dieses Problems wird empfohlen, alle Front-End-Server vor der Aktualisierung von Back-End-Servern zu aktualisieren.

Stellen Sie außerdem vor dem Aktualisieren sicher, dass die erforderlichen Dienste ausgeführt werden. Installieren und aktivieren Sie vor der Ausführung des Exchange-Setups Network News Transfer Protocol (NNTP), SMTP, W3SVC und IIS Admin (Starten nicht unbedingt erforderlich). Bei Deaktivierung der Dienste MSExchangeMTA, IMAP4, POP3 und MSExchangeIS wird das Setup nicht ausgeführt. Diese Dienste werden allerdings nach dem Starten des Setups aktiviert. Nach Abschluss des Setups können Sie alle nicht benötigten Dienste deaktivieren.

Szenarien für die Bereitstellung einer Front-End- und Back-End-Topologie

In diesem Thema werden allgemeine Szenarien für die Bereitstellung einer Exchange-Front-End- und Back-End-Topologie erläutert. Die Szenarien können in zwei Kategorien unterteilt werden: Intranet- und Extranetszenarien. Der Fokus der Intranetszenarien liegt auf der Leistung und Skalierbarkeit, wobei die Extranetszenarien auf Sicherheit zugeschnitten sind.

In allen Szenarien werden die folgenden Themen erläutert:

- Szenario Um welches Szenario handelt es sich, und wann wird es eingesetzt?
- Setupanweisungen Wie wird das Szenario eingerichtet? Allgemeine Anweisungen. (Spezielle Konfigurationsanweisungen werden zu einem späteren Zeitpunkt behandelt.)
- Diskussion Was ist das Besondere an diesem Szenario? Wie funktioniert es? Welche zusätzlichen Informationen werden benötigt, um dieses Szenario beurteilen zu können?
- Aspekte Vorbehalte oder Beschränkungen dieses Szenarios.

Alle vier Szenarien benötigen eine Firewall. Sie können Software- und Hardwarelösungen als Firewall einsetzen. Die Anschlussfilterung gilt als Minimalanforderung für eine Firewall, die den Server vor dem Internet schützt.

Erweiterte Firewall in einem Umgebungsnetzwerk

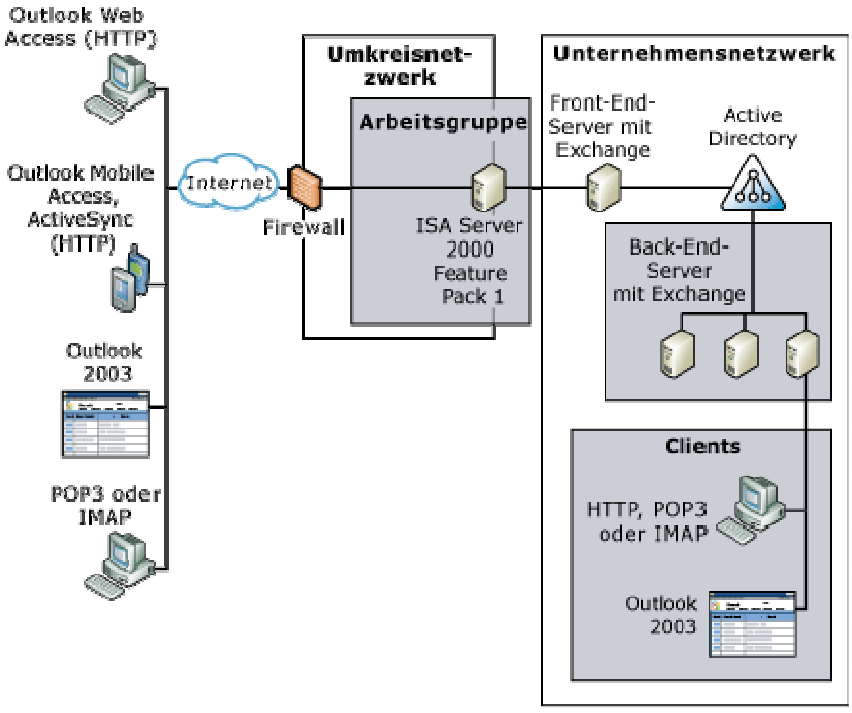
In der folgenden Abbildung wird ein erweitertes Firewallszenario dargestellt, in dem eine erweiterte Firewall innerhalb eines Umgebungsnetzwerk zwischen die Internetfirewall und die interne Firewall platziert wurde. Front-End- und Back-End-Server befinden sich in demselben Netzwerk hinter der internen Firewall. Aus folgenden Gründen handelt es sich hierbei um die empfohlene Topologie:

- Mehr Sicherheit, da Eindringlinge vom Rest des Netzwerk isoliert werden.
- Filtern von Anwendungsprotokollen.
- Zusätzliche Überprüfung von Anfragen, bevor diese über Proxy an das interne Netzwerk weitergeleitet werden.

Hinweis:

Alternativ zur Platzierung des erweiterten Firewallservers innerhalb eines Umgebungsnetzwerks hinter einer separaten Firewall kann der erweiterte Firewallserver selbst als Internetfirewall eingesetzt werden.

Exchange-Front-End-Server hinter einer erweiterten Firewall



Szenario

Ein Unternehmen platziert eine erweiterte Firewall, wie z. B. ISA Server, zwischen zwei separate Firewalls. Die Entscheidung des Unternehmens, diese erweiterte Firewalltopologie einzurichten, basiert auf den folgenden Vorteilen:

- Erweiterte Firewall bieten zusätzliche Netzwerksicherheit durch den Schutz vor unerlaubtem Zugriff und die Überprüfung des Datenverkehrs. Weiterhin wird der Netzwerkadministrator vor Angriffen gewarnt.
- Erweiterte Firewalls ermöglichen die Verwendung der Anschlussfilterung sowie der IP-Filterung, um den Datenverkehr zu steuern.
- Mit erweiterten Firewalls können Sie den Zugriff nach Benutzern, Gruppen, Anwendungstyp, Tageszeit, Inhalt sowie Zielen beschränken.

Setupanweisungen

Ausführliche Setupanweisungen finden Sie unter Einrichten einer Front-End- und Back-End-Topologie mit einer erweiterten Firewall in einem Umgebungsnetzwerk. Weitere Informationen zu ISA Server mit Produktinformationen und Angaben zu technischen Ressourcen finden Sie auf der ISA Server-Website.

Diskussion

ISA Server beinhaltet zwei Regeltypen:

- Serververöffentlichungsregeln Diese Regeln, die für alle Protokolle gelten, überprüfen eingehende Anfragen am Eingangsanschluss. Wenn eine eingehende Anfrage zugelassen ist, wird sie von der Protokollregel vom Eingangsanschluss zu einer internen IP-Adresse weitergeleitet.
- Webveröffentlichungsregeln Diese Regeln gelten nur für HTTP- oder HTTPS (80/443)-Anfragen. Sie können Webveröffentlichungsregeln zum Filtern von eingehenden Anfragen basierend auf dem Diensttyp, Anschluss und dem Namen des Quell- und Zielcomputers verwenden. Sie können ebenfalls nur bestimmte Server zulassen bzw. Server mit hohem Risiko verweigern.

Wenn Sie HTTP-Clients unterstützen, erstellen Sie eine Webveröffentlichungsregel für HTTP- oder HTTPS-Datenverkehr. Wenn Sie POP- oder IMAP-Clients unterstützen, erstellen Sie Serververöffentlichungsregeln, um diese Protokolle zu verarbeiten.

Im Gegensatz zum Umgebungsnetzwerkszenario muss der ISA-Server im Umgebungsnetzwerk kein Mitgliedsserver sein, es sei denn, Sie konfigurieren ISA Server für die Authentifizierung von Anfragen. Grundsätzlich gilt, dass Sie ISA Server zur Authentifizierung von Benutzern nicht konfigurieren müssen, wenn die Authentifizierung auf dem Front-End-Server konfiguriert ist. Wenn Sie jedoch eingehende Anfragen auf bestimmte Benutzer beschränken möchten, müssen Sie eine Webveröffentlichungsregel erstellen, die die Benutzer angibt und Authentifizierung auf dem ISA Server ermöglicht. In diesem Fall muss der ISA-Server Mitglied der Windows-Domäne sein. ISA Server leitet die Anmeldeinformationen des Benutzers nicht an die Back-End-Server weiter. Benutzer können daher nicht für Outlook Web Access vorauthentifiziert werden, obwohl ISA Server Benutzer authentifizieren und den Zugriff auf das Netzwerk beschränken kann.

Aspekte

Im erweiterten Firewallszenario ist der RPC-Zugriff auf das interne Netzwerk nicht erforderlich. Dies wird häufig als Vorteil betrachtet, da auf der internen Firewall weniger Anschlüsse geöffnet werden müssen. Unabhängig von der Anzahl der geöffneten Anschlüsse besteht jedoch ein Sicherheitsrisiko. Um dieses Sicherheitsrisiko zu vermeiden, stellen Sie sicher, dass die richtigen Filter für die geöffneten Anschlüsse festgelegt sind.

Im erweiterten Firewallszenario haben Sie zwei Möglichkeiten zur Konfiguration von SSL:

- Nur zwischen dem Client und dem ISA-Server.
- Zwischen dem Client und dem ISA-Server und zwischen dem ISA-Server und dem Front-End-Server.

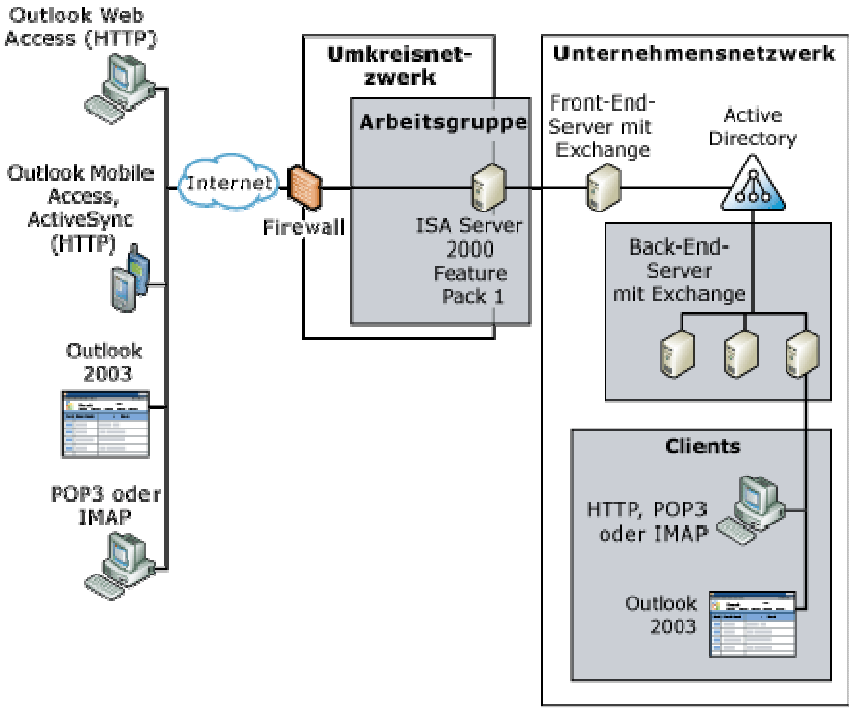
Die zweite Option wird normalerweise verwendet, wenn eine Kundenrichtlinie die Verschlüsselung von E-Mail-Vekehr innerhalb des Umgebungsnetzwerks vorschreibt. Wenn der ISA-Server die SSL-Anfrage vom Client empfängt, beendet er die Sitzung und eröffnet eine neue SSL-Sitzung mit einem neuen Zertifikat, um den Front-End-Server zu kontaktieren. Der Name der einzelnen Zertifikate ist sehr wichtig. Der Zertifikatsname der eingehenden Anfrage muss mit dem Namen übereinstimmen, die der Benutzer im URL eingegeben hat. Weiterhin muss der Zertifikatsname der Anfrage an den Front-End-Server mit dem Namen oder der IP-Adresse des Front-End-Servers übereinstimmen.

Verwenden Sie zum Konfigurieren von SSL in ISA Server die Registerkarte **Bridging** in der Webveröffentlichungs-Serverregel, um den SSL-Datenverkehr zu lenken. Wenn Sie mehrere Domänen hosten und SSL verwenden möchten, müssen Sie einen Listener und verschiedene IP-Adressen für jede einzelne Domäne einrichten. Die Zertifikate müssen so benannt werden, dass sie den Zielnamen oder IP-Adressen entsprechen.

Einrichten einer Front-End- und Back-End-Topologie mit einer erweiterten Firewall in einem Umgebungsnetzwerk

Sie können eine Front-End- und Back-End-Topologie mit einer erweiterten Firewall. In der folgenden Abbildung wird das Front-End- und Back-End-Szenario mit einer erweiterten Firewall dargestellt. In diesem Szenario platzieren Sie den erweiterten Firewallserver innerhalb des Umgebungsnetzwerks und zwischen die Internetfirewall und die interne Firewall. Sie platzieren Front-End- und Back-End-Server im gleich Netzwerk hinter der internen Firewall.

Exchange-Front-End-Server hinter einer erweiterten Firewall



Bevor Sie beginnen

Bevor Sie das in diesem Thema beschriebene Verfahren durchführen, lesen Sie bitte die folgenden Abschnitte:

- Szenarien für die Bereitstellung einer Front-End- und Back-End-Topologie
- Verwenden von ISA Server 2000 mit Exchange Server 2003

Verfahren

So richten Sie eine Front-End- und Back-End-Topologie mit einer erweiterten Firewall in einem Umgebungsnetzwerk ein

1. Befindet sich eine Firewall oder ein Anschlussfilter vor der erweiterten Firewall, konfigurieren Sie diese für Clientprotokolle und eingehende Anschlüsse: 443 (SSL HTTP), 993 (SSL POP3), 995 (SSL IMAP4) sowie für alle anderen Anschlüsse für eingehenden Datenverkehr (z. B. kann der SMTP-Datenverkehr durch diese Firewall ebenfalls erforderlich sein). Diese Firewall sollte den Zugriff auf bestimmte erweiterte Firewallserver beschränken.
2. (Optional) Wenn Sie eine Intranetfirewall zwischen der erweiterten Firewall und dem

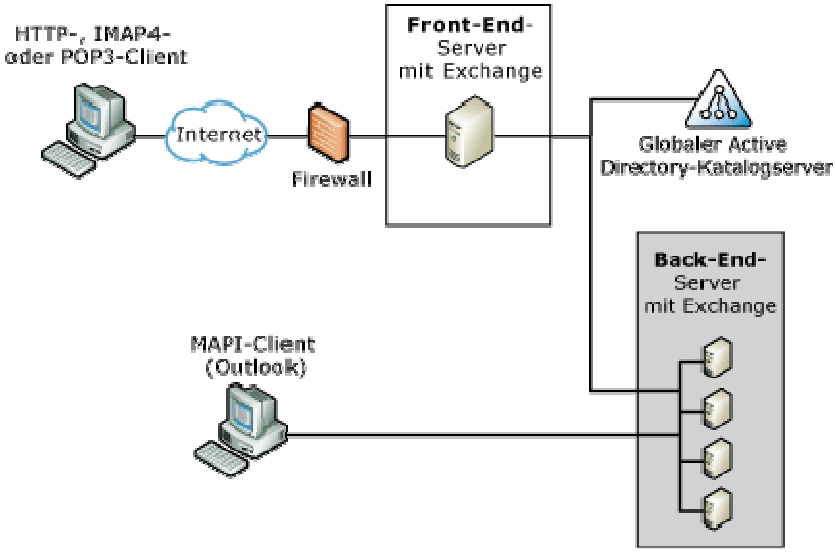
Intranet einsetzen, konfigurieren Sie die Intranetfirewall zur Öffnung bestimmter Anschlüsse, um den erforderlichen Netzwerkverkehr vom erweiterten Firewallserver (z. B. ein Server unter Microsoft® Internet Security und Acceleration (ISA) Server) zum Intranet zu unterstützen. Dabei würde es sich um ein beliebiges von der erweiterten Firewall über Proxy weitergeleitetes Protokoll handeln: Anschlüsse 40 oder 80 (je nach dem, ob die erweiterte Firewall SSL-Verschlüsselung unterstützt), 993 und 994. Weiterhin muss die Intranetfirewall Zugriff auf alle anderen Protokolle gewähren, die vom erweiterten Firewallserver je nach Tasks und Konfiguration benötigt werden. Dazu zählen unter Umständen Authentifizierung, DNS (Domain Name System) und Active Directory-Zugriff. Die genaue Liste richtet sich nach dem Sicherheitsstandard und den vom jeweiligen Unternehmen implementierten Features.

3. Konfigurieren Sie die erweiterte Firewall. Beachten Sie die folgenden allgemeinen Richtlinien, wenn Sie einen ISA-Server in einer Front-End- und Back-End-Topologie bereitstellen. (Detaillierte Informationen zum Konfigurieren von ISA Server finden Sie in der Produktdokumentation.)
   a. Konfigurieren Sie einen Listener für SSL.
   b. Erstellen Sie ein Zielset mit der externen IP-Adresse des ISA-Servers. Dieses Zielset wird in der Web-Veröffentlichungsregel festgelegt.
   c. Erstellen Sie eine Web-Veröffentlichungsregel, die die Anfragen an den internen Front-End-Server umleitet.
   d. Erstellen Sie Protokollregeln, um die Anschlüsse in ISA Server für ausgehenden Datenverkehr zu öffnen.
4. Konfigurieren Sie den ISA-Server für Microsoft Office Outlook® Web Access. (Informationen zum Konfigurieren eines ISA-Servers für Outlook Web Access finden Sie im Microsoft Knowledge Base-Artikel 307347, "Sichere OWA-Veröffentlichung hinter ISA Server kann benutzerdefinierten HTTP-Header erfordern.")

Front-End-Server hinter einer Firwall

In der folgenden Abbildung wird eine Front-End- und Back-End-Topologie dargestellt, in der sich der Front-End-Server hinter einer Firewall befindet.

Eine einfache Exchange-Firewalltopologie



Szenario

Die Entscheidung eines Unternehmens, das Exchange-System hinter einer firmeninternen Firewall zu platzieren, hat folgende Gründe: Gewährleistung von Sicherheit und Zugriff auf Outlook Web Access, POP oder IMAP über das Internet.

Setupanweisungen

Ausführliche Setupanweisungen finden Sie unter Einrichten einer Front-End- und Back-End-Topologie mit einem Front-End-Server hinter einer Firewall.

Diskussion

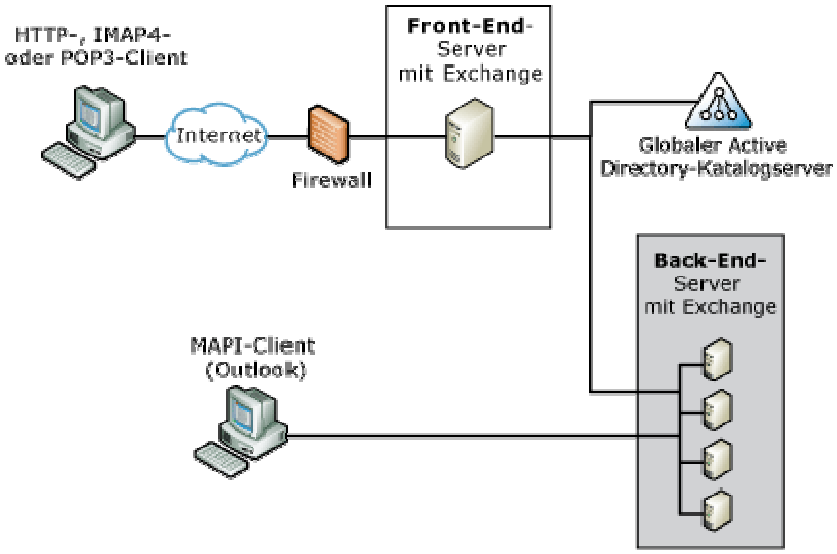
Da sich die gesamte Konfiguration innerhalb der Firewall befindet, ist für Exchange keine spezielle Konfiguration erforderlich. Nachdem eine Anfrage über die Firewall an den Front-End-Server weitergeleitet wird, gibt der Front-End-Server eine Antwort ohne Konfigurationsänderungen zurück.

Die IP-Adressfilterung wird dringend empfohlen, um die Anfragen über die Firewall auf die Front-End-Server zu beschränken, auf denen Exchange ausgeführt wird und die Anfragen über die Firewall an andere Server innerhalb der Organisation blockieren.

Einrichten einer Front-End- und Back-End-Topologie mit einem Front-End-Server hinter einer Firewall

Sie können eine Front-End- und Back-End-Topologie mit einem Front-End-Server hinter einer Firewall einrichten. In der folgenden Abbildung wird das Front-End- und Back-End-Szenario mit einem Front-End-Server hinter einer Firewall dargestellt.

Eine einfache Exchange-Firewalltopologie



Bevor Sie beginnen

Bevor Sie das in diesem Thema beschriebene Verfahren durchführen, lesen Sie bitte die folgenden Abschnitte:

- Szenarien für die Bereitstellung einer Front-End- und Back-End-Topologie
- Verwenden von ISA Server 2000 mit Exchange Server 2003

Verfahren

So richten Sie eine Front-End- und Back-End-Topologie mit einem Front-End-Server hinter einer Firewall ein

1. Richten Sie eine Exchange-Front-End- und Back-End-Standardumgebung in Ihrem Unternehmen ein. Weitere Informationen zu Exchange-Front-End- und Back-End-

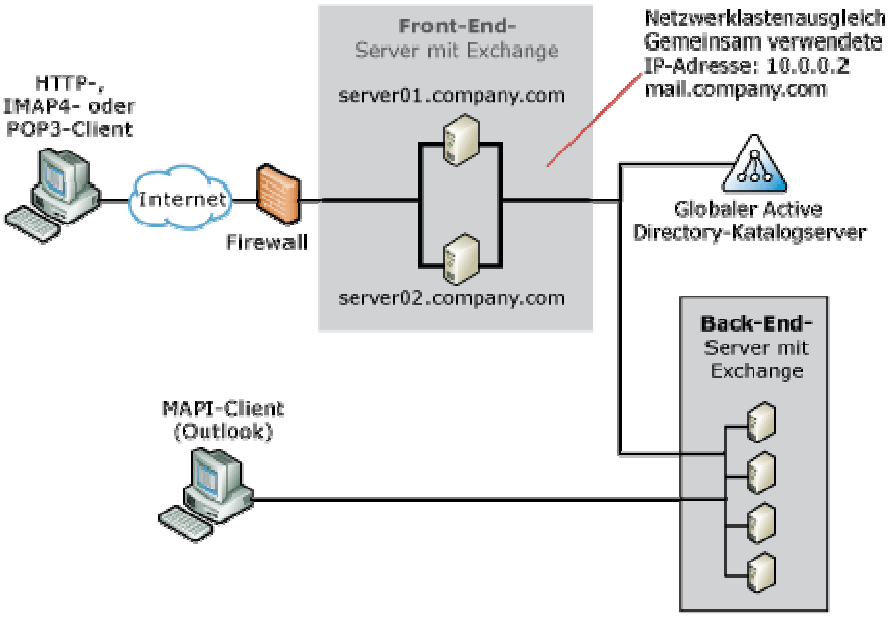
Standardumgebungen finden Sie unter Einführung in die Front-End- und Back-End-Topologien für Exchange Server 2003 und Exchange 2000 Server. Weitere Informationen zum Festlegen eines Front-End-Servers finden Sie unter Festlegen eines Front-End-Servers.

2. Konfigurieren Sie eine Firewall zwischen dem Front-End-Server und dem Internet. Weitere Informationen zum Konfigurieren einer Internetfirewall für den Einsatz eines Front-End-Servers unter Exchange finden Sie unter Konfigurieren von Firewalls.

Webfarm mit einer Firewall

In der folgenden Abbildung wird ein Webfarmszenario dargestellt

Front-End- und Back-End-Topologie in einer Webfarm



Szenario

Ein Unternehmen stellt 200.000 Benutzern Outlook Web Access bereit. Ziel ist die Verwendung eines einzelnen Namespace (zum Beispiel https://mail), mit dem alle Benutzer auf ihre Postfächer zugreifen können. Aus Gründen der Systemleistung möchte das Unternehmen zudem einen Engpass auf dem Front-End-Server oder einen einzelnen Fehlerpunkt vermeiden und die Datenlast unter Verwendung von NLB (Network Load

Balancing, Netzwerklastenausgleich) über mehrere Front-End-Server verteilen. Dieses Szenario wird als "Webfarm" bezeichnet.

Hinweis:

Obwohl es sich hierbei um das einzige Szenario handelt, in dem NLB geschildert wird, können Sie NLB für den Lastenausgleich auf Front-End-Servern in allen in diesem Handbuch beschriebenen Szenarien verwenden.

Setupanweisungen

Ausführliche Anweisungen finden Sie unter Einrichten einer Front-End- und Back-End-Topologie mit einer Webfarm hinter einer Firewall.

Diskussion

Informationen zum Einrichten von Lastenausgleich finden Sie in der Windows-Onlinedokumentation. Zur Konfiguration von Exchange auf Front-End-Servern sind keine speziellen Schritte erforderlich.

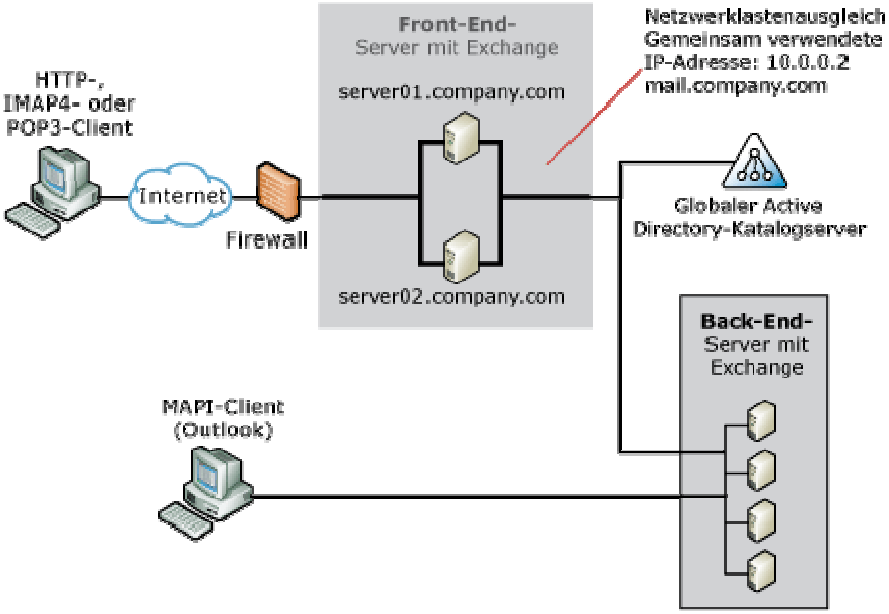
Aspekte

Wie zuvor bereits erwähnt können Sie mit der Lastenausgleichslösung sicherstellen, dass alle Benutzer innerhalb einer Sitzung immer zu demselben Front-End-Server geleitet werden.

Einrichten einer Front-End- und Back-End-Topologie mit einer Webfarm hinter einer Firewall

Sie können eine Front-End- und Back-End-Topologie mit eine Webfarm hinter einer Firewall erstellen. In der folgenden Abbildung wird das Front-End- und Back-End-Szenario mit einer Webfarm hinter einer Firewall dargestellt. In diesem Szenario verteilen Sie die Front-End-Serverlast über mehrere Front-End-Server. Sie platzieren mehrere Front-End-Server hinter einer Firewall.

Front-End- und Back-End-Topologie in einer Webfarm



Bevor Sie beginnen

Bevor Sie das in diesem Thema beschriebene Verfahren durchführen, lesen Sie bitte die folgenden Abschnitte:

- Szenarien für die Bereitstellung einer Front-End- und Back-End-Topologie
- Verwenden von ISA Server 2000 mit Exchange Server 2003

Verfahren

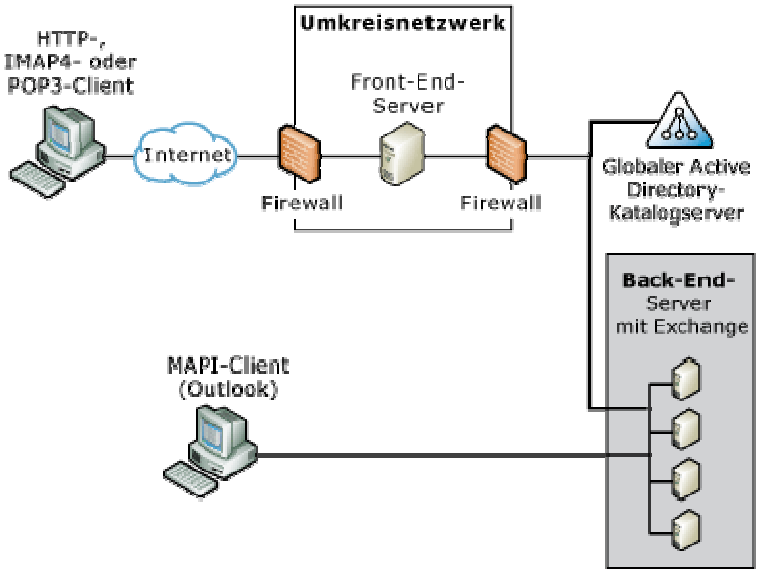
So richten Sie eine Front-End- und Back-End-Topologie mit einer Webfarm hinter einer Firewall ein

1. Richten Sie eine Gruppe von Servern als Back-End-Server in derselben Struktur ein.
2. Verteilen Sie die Benutzer auf die Server.
3. Richten Sie eine andere Servergruppe als Front-End-Server ein, und konfigurieren Sie Netzwerklastenausgleich auf allen Servern.

Front-End-Server in einem Perimeternetzwerk

In der folgenden Abbildung wird ein Exchange-Front-End-Server in einem Umkreisnetzwerk dargestellt.

Exchange-Front-End-Server in einem Umkreisnetzwerk



Szenario

In dieser Abbildung platziert das Unternehmen den Front-End-Server zwischen zwei getrennte Firewalls. Die erste Firewall trennt den Front-End-Server vom Internet und erlaubt Anfragen nur zu diesem Front-End-Server. Die zweite Firewall trennt den Front-End-Server vom internen Netzwerk. Die Systeme zwischen den beiden Firewalls liegen in einem so genannten Umkreisnetzwerk (auch als entmilitarisierte Zone (DMZ) oder überwachtes Subnetz bezeichnet). Eine Umkreisnetzwerkkonfiguration bietet mehr Sicherheit, da bei Ausfall des Front-End-Servers eine weitere Barriere zwischen dem Eindringling und dem Rest des Netzwerk besteht.

Hinweis:

Die Platzierung der Front-End-Server innerhalb des Umkreisnetzwerks stellt eine Methode für die Bereitstellung der Front-End- und Back-End-Topologie innerhalb eines Umkreisnetzwerks dar. Empfohlen wird jedoch die im ersten Szenario Erweiterte Firewall in einem Umgebungsnetzwerk dargelegte Methode. Bei dieser Methode werden die Front-End- und Back-End-Server innerhalb des Intranets und

die erweiterte Firewall (wie beispielsweise ISA Server) im Umkreisnetzwerk platziert. Mit der erweiterten Firewall können Anwendungsprotokolle gefiltert und zusätzliche Authentifizierungen für Anfragen durchgeführt werden, bevor eine Zwischenspeicherung im internen Netzwerk erfolgt.

Setupanweisungen

Ausführliche Setupanweisungen finden Sie unter Einrichten einer Front-End- und Back-End-Topologie mit einem Front-End-Server in einem Perimeternetzwerk.

Diskussion

In Unternehmen, in denen ein Umkreisnetzwerk standardmäßig eingesetzt wird, wird der Netzwerkverkehr in der Regel über die Internetfirewall durch Beschränkung der auf der Internetfirewall aktivierten Netzwerkanschlüsse gesteuert. Für den uneingeschränkten Betrieb eines Front-End-Servers müssen jedoch bestimmte Anschlüsse geöffnet sein.

Aspekte

Einige Unternehmen, die Umkreisnetzwerktopologien für andere Dienste verwenden, wenden Richtlinien an, die Computer innerhalb des Umkreisnetzwerks daran hindern, Verbindungen zu Servern im Unternehmensintranet herzustellen. Ein Front-End-Server unter Exchange wird in dieser Konfiguration nicht unterstützt, da er Verbindungen herstellen muss.

Weiterhin muss der Front-End-Server Mitglied derselben Windows-Gesamtstruktur wie die Back-End-Server sein. In einigen Unternehmen sind Mitgliedsserver im Umkreisnetzwerk nicht erlaubt. Daher stellt der Einsatz eines Front-End-Servers im Umkreisnetzwerk für diese Unternehmen keine Option dar.

Der Front-End-Server sollte vor Inbetriebnahme der Intranetfirewall vollständig konfiguriert sein. Für die Konfigurationseinstellungen auf dem Front-End-Server im Exchange-System-Manager ist die Ausführung des Systemaufsichtsdienstes (MSExchangeSA) erforderlich, damit die Konfigurationsinformationen in der Metabase repliziert werden können. Der MSExchangeSA-Dienst benötigt RPC-Zugriff auf die Back-End-Server, wobei RPC-Datenverkehr über eine Intranetfirewall in einem Umkreisnetzwerk oft nicht erlaubt sind.

Die DSAccess-Komponente in Exchange 2000 Server SP2 wurde überarbeitet, um den Support für Umkreisnetzwerke zu verbessern, in denen RPC-Datenverkehr über die Internetfirewall nicht erlaubt ist. Es werden jedoch zwei zusätzliche Registrierungsschlüssel bereitgestellt, die festgelegt auf dem Front-End-Server festgelegt werden sollten, um NetLogon und die Ping-Funktion des Verzeichniszugriffs zu deaktivieren:

- **NetLogon** DSAccess stellt eine Verbindung zu Active Directory-Servern her, um den verfügbaren Speicherplatz, die Synchronisierungsdauer sowie die Replikationsteilnahme

unter Verwendung des NetLogon-Dienstes mit RPC zu überprüfen. Wenn Sie RPC-Datenverkehr über die interne Firewall nicht zulassen möchten, sollten Sie die NetLogon-Überprüfung beenden, indem Sie den DisableNetlogonCheck-Schlüssel auf dem Front-End-Server erstellen.

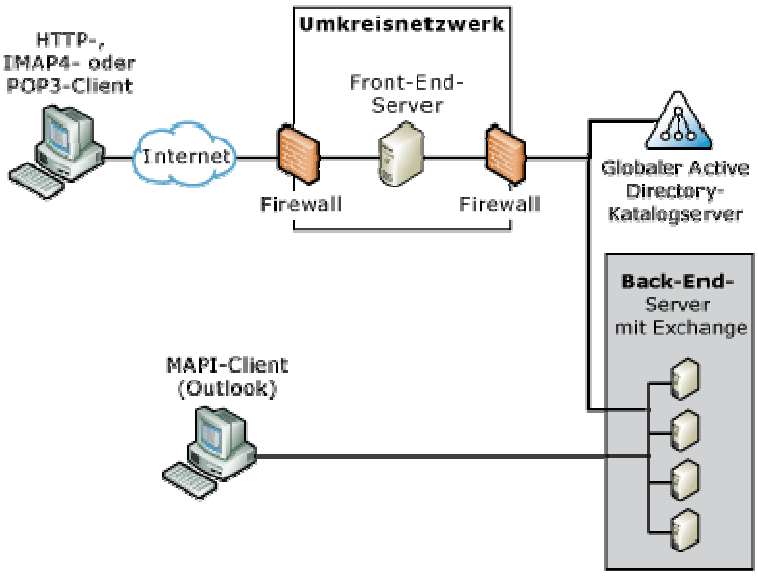
- **Verzeichniszugriffs-Ping** Standardmäßig "pingt" der Verzeichniszugriff jeden Server mit dem ICMP-Protokoll (Internet Control Message Protocol) an, um die Verfügbarkeit zu überprüfen. In einem Umkreisnetzwerk ohne ICMP-Konnektivität zwischen dem Server unter Exchange und den Domänencontrollern legt der Verzeichniszugriff jedoch fest, das kein Domänencontroller verfügbar ist. Der Verzeichniszugriff verwirft dann die alten Topologien und führt häufig neue Topologieanalysen durch, wodurch die Serverleistung beeinträchtigt wird. Deaktivieren Sie zur Vermeidung dieser Leistungsprobleme den Verzeichniszugriffs-Ping auf dem Front-End-Server, indem Sie den LdapKeepAliveSecs-Registrierungsschlüssel für die Windows-Implementierung von LDAP (wLDAP) erstellen.

Informationen zum Festlegen von Registrierungsschlüsseln finden Sie unter Konfigurieren von DSAccess für Perimeternetzwerke.

Einrichten einer Front-End- und Back-End-Topologie mit einem Front-End-Server in einem Perimeternetzwerk

Sie können eine Front-End- und Back-End-Topologie mit einem Front-End-Server in einem Umkreisnetzwerk erstellen. In der folgenden Abbildung wird das Front-End- und Back-End-Szenario mit einem Front-End-Server in einem Umkreisnetzwerk dargestellt. In diesem Szenario platzieren Sie den Front-End-Server zwischen die Internetfirewall und die interne Firewall.

Exchange-Front-End-Server in einem Umkreisnetzwerk



Bevor Sie beginnen

Bevor Sie das in diesem Thema beschriebene Verfahren durchführen, lesen Sie bitte die folgenden Abschnitte:

- Szenarien für die Bereitstellung einer Front-End- und Back-End-Topologie
- Verwenden von ISA Server 2000 mit Exchange Server 2003

Verfahren

So richten Sie eine Front-End- und Back-End-Topologie mit einem Front-End-Server in einem Umkreisnetzwerk ein

1. Konfigurieren Sie die äußere Firewall (Internet) für eine Firewall in dieser Umgebung, und beschränkten Sie den Zugriff auf die erforderlichen Anschlüsse und auf einen bestimmten Front-End-Server.
2. Konfigurieren Sie die innere Firewall (Intranet) so, dass lediglich bestimmte Anschlüsse für die Authentifizierung, DNS und Active Directory-Zugriff geöffnet sind. Die genaue Liste richtet sich nach dem Sicherheitsstandard und den vom jeweiligen Unternehmen ausgewählten Features.

Weitere Informationen

Informationen zum Konfigurieren von Internet- und Intranetfirewalls finden Sie unter Konfigurieren von Firewalls.

Konfigurieren von Exchange-Front-End-Servern

Ein Front-End-Server ist zunächst einmal ein gewöhnlicher Exchange-Server, bis er entsprechend konfiguriert wird. Ein Front-End-Server muss keine Benutzer oder Öffentliche Ordner hosten.

Ein Front-End-Server muss Mitglied derselben Exchange-Organisation wie die Back-End-Server sein (daher ein Mitglied derselben Windows®-Struktur).

Ausführliche Anweisungen zum Festlegen eines Exchange-Servers als Front-End-Server finden Sie unter Festlegen eines Front-End-Servers.

Festlegen eines Front-End-Servers

Ein Front-End-Server ist ein Exchange-Server, der Anforderungen von Clients empfängt und diese mithilfe der Proxyfunktion zur Verarbeitung an den entsprechenden Back-End-Server weiterleitet.

Bevor Sie beginnen

Zum erfolgreichen Durchführen der Verfahren dieses Themas müssen folgende Voraussetzungen erfüllt sein:

- Der als Front-End-Server bestimmte Server gehört derselben Microsoft® Windows®-Gesamtstruktur an wie die Back-End-Server.
- Der als Front-End-Server bestimmte Server gehört derselben Exchange-Organisation an wie die Back-End-Server.

Verfahren

So legen Sie einen Front-End-Server fest

1. Installieren Sie den Server, auf dem Exchange Server in der Organisation ausgeführt werden soll.

Hinweis:

Mit Exchange 2000 Server können nur Enterprise Edition-Server als Front-End-Server konfiguriert werden. In Exchange Server 2003 können sowohl Standard Edition- als auch Enterprise Edition-Server als Front-End-Server konfiguriert werden.

2. Wechseln Sie mithilfe von **Exchange-System-Manager** zum Serverobjekt, klicken Sie mit der rechten Maustaste auf das Serverobjekt, und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie **Dies ist ein Front-End-Server** aus, und schließen Sie dann die Seite.
4. Zum Verwenden des Front-End-Servers führen Sie einen der folgenden Schritte aus:
   - Starten Sie den Computer neu.
   - Beenden Sie die HTTP-, POP3- und IMAP4-Dienste, und starten Sie sie neu.
5. Die virtuellen Exchange-Standardverzeichnisse sind nun konfiguriert. Es wird empfohlen, zusätzlich SSL zu konfigurieren. Ausführliche Anweisungen zum Konfigurieren von SSL für POP3, IMAP4 und SMTP finden Sie in „How to Configure SSL for POP3, IMAP4, and SMTP“ (nur auf Englisch verfügbar) unter Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Server Topology Guide. Ausführliche Anweisungen zum Konfigurieren von SSL für HTTP finden Sie in „How to Configure SSL for HTTP“ (nur auf Englisch verfügbar) unter Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Server Topology Guide.

Weitere Informationen

- Weitere Informationen finden Sie in:
  - „Configuring Exchange Front-end Servers“ (nur auf Englisch verfügbar) unter Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Server Topology Guide
  - „How to Set Up a Front-End and Back-End Topology with a Front-End Server Behind a Firewall“ (nur auf Englisch verfügbar) unter Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Server Topology Guide
  - Exchange Server 2003 Client Access Guide

Erstellen von virtuellen HTTP-Servern

Verwenden Sie den Exchange-System-Manager beim Erstellen von virtuellen Servern und nicht den Internetdienste-Manager. Wenn Sie virtuelle Server im Exchange-System-Manager

erstellen, müssen Sie den URL nicht vereinfachen. Nach dem Erstellen eines auf Postfächer gerichteten virtuellen Servers und dem Festlegen von Hostheadern können Benutzer **http://<virtueller Servername>/** ohne die Angabe von /**exchange** eingeben.

Ausführliche Anweisungen zum Erstellen eines virtuellen HTTP-Servers finden Sie unter Erstellen eines virtuellen Servers.

Im IP-Adressfeld können Sie die Standardeinstellung **Alle nicht zugewiesen** verwenden oder diese auf eine bestimmte dem Server zugewiesene IP-Adresse beschränken. Wenn SSL für die Verbindung zu diesem Front-End-Server verwendet wird, möchten Sie vielleicht eine bestimmte IP-Adresse für den virtuellen Server konfigurieren.

Erstellen eines virtuellen Servers

Verwenden Sie dieses Verfahren zum Erstellen eines virtuellen Servers.

Verfahren

So erstellen Sie eine virtuellen Server

1. Klicken Sie im Container für HTTP-Protokolle im Exchange-System-Manager mit der rechten Maustaste auf **HTTP**, und wählen Sie dann **Neuer virtueller Server**.

   Hinweis:

   Für einen Namen wird folgende Eingabeform empfohlen: "adatum.com (front-end)". Durch die konsistente Benennung von neuen virtuellen Servern wird sichergestellt, dass der Zweck und die zugewiesene Domäne der einzelnen virtuellen Server leicht erkannt werden kann. Der Name des virtuellen Server wird nur für Identifikationszwecke verwendet und wirkt sich nicht auf den Betrieb aus.

2. Klicken Sie auf **Postfächer** oder **Öffentlicher Ordner**, klicken Sie auf **Ändern**, und führen Sie dann eine der folgenden Aktionen aus:

   - Wenn der virtuelle Server auf Postfächer verweist, wählen Sie die Domäne aus.

     Hinweis:

     Die Liste der Domänen unter **SMTP-Domäne auswählen** wird von den Domänen der SMTP-Adressen in den Exchange-Empfängerrichtlinien der Organisation abgerufen. Wenn mehrere Empfängerrichtlinien für dieselbe Domäne vorhanden sind, werden in diesem Dialogfeld Duplikate angezeigt. Die Auswahl der Domäne ist dabei unerheblich.

   - Wenn der virtuelle Server auf einen Öffentlichen Ordner verweist, wählen Sie

den Öffentlichen Ordner aus, der als Stammverzeichnis des Öffentlichen Ordners für diesen virtuellen Server agieren soll.

3. Klicken Sie auf **Erweitert**, und fügen Sie die Hostheader hinzu, die alle Namen festlegen, die ein Client möglicherweise für den Verbindungsaufbau zu diesem Front-End-Server verwendet.

   Hinweis:

   Wenn ein Front-End-Server intern und extern verwendet wird, wird sowohl die Angabe eines Hostnamens als auch diejenige eines vollständig qualifizierten Domänennamens empfohlen.

Konfigurieren der Authentifizierung

Die duale Authentifizierung wird dringend empfohlen, bei der sowohl die Front-End- als auch die Back-End-Server zur Authentifizierung von Benutzern konfiguriert werden. Standardmäßig werden Front-End-Server zur Durchführung der dualen Authentifizierung konfiguriert.

Wenn Sie jedoch über ein eingeschränktes Umgebungsnetzwerk verfügen, in dem RPCs über die Intranetfirewall nicht erlaubt sind und der Front-End-Server Benutzer nicht authentifizieren kann, können Sie Pass-Through-Authentifizierung verwenden.

Hinweis:

Bei der Pass-Through-Authentifizierung werden anonyme HTTP-Anfragen direkt an den Back-End-Server geleitet und authentifiziert. Verwenden Sie die Pass-Through-Authentifizierung nur, wenn der Front-End-Server Benutzer nicht authentifizieren kann. Weitere Informationen finden Sie unter Szenarien für die Bereitstellung einer Front-End- und Back-End-Topologie.

Ausführliche Anweisungen zur Konfiguration der Authentifizierung auf einem Front-End-Server finden Sie unter Konfigurieren der Authentifizierung auf einem Front-End-Server.

Konfigurieren der Authentifizierung auf einem Front-End-Server

Sie können Ihren Front-End-Server für die duale Authentifizierung oder für die Pass-Through-Authentifizierung konfigurieren. Bei der dualen Authentifizierung werden sowohl die Front-End- als auch die Back-End-Server zur Authentifizierung von Benutzern konfiguriert. Wenn Sie jedoch über ein eingeschränktes Umgebungsnetzwerk verfügen, in dem RPCs über die

Intranetfirewall nicht erlaubt sind und der Front-End-Server Benutzer nicht authentifizieren kann, können Sie Pass-Through-Authentifizierung verwenden.

Bevor Sie beginnen

Zum erfolgreichen Durchführen der Verfahren dieses Themas müssen folgende Voraussetzungen erfüllt sein:

- Verwenden Sie die Pass-Through-Authentifizierung nur, wenn der Front-End-Server Benutzer nicht authentifizieren kann.
- Sie haben das Thema Szenarien für die Bereitstellung einer Front-End- und Back-End-Topologie gelesen.

Verfahren

So konfigurieren Sie die Authentifizierung auf einem Front-End-Server

1. Klicken Sie auf **Start**, zeigen Sie auf **Programme**, zeigen Sie auf **Microsoft Exchange**, und klicken Sie dann auf **System-Manager**.
2. Navigieren Sie zum virtuellen Verzeichnis "Exchange" oder "Öffentlich".
3. Klicken Sie mit der rechten Maustaste auf das virtuelle Exchange-Verzeichnis "Exchange" oder "Öffentlich", und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Zugriff**, und klicken Sie dann auf **Authentifizierung**.
5. Führen Sie einen der folgenden Schritte durch:
   - Aktivieren Sie zum Konfigurieren des Front-End-Servers zur Authentifizierung von Benutzern (wie bei der dualen Authentifizierung) das Kontrollkästchen **Standardauthentifizierung**.
   - Aktivieren Sie zur Konfiguration der Pass-Through-Authentifizierung das Kontrollkästchen **Anonymer Zugriff**, und deaktivieren Sie dann das Kontrollkästchen **Standardauthentifizierung**.

Konfigurieren eines Front-End-Servers als Standarddomäne

Sie können einen Front-End-Server als Standarddomäne konfigurieren, damit sich Benutzer ihre Domäne nicht merken müssen.

Nach Abschluss der Replikation können sich Benutzer lediglich mit ihrem Benutzernamen und ihrem Kennwort anmelden. Die Angabe der Domäne ist nicht erforderlich.

Ausführliche Anweisungen zur Konfiguration eines Front-End-Servers als Standarddomäne finden Sie unter Konfigurieren eines Front-End-Servers als Standarddomäne.

Konfigurieren von formularbasierter Authentifizierung für Exchange Server 2003

Für Exchange Server 2003 können Sie die neue Funktion zur formularbasierten Authentifizierung für Ihre Microsoft® Office Outlook® Web Access-Clients aktivieren.

Wichtig:

In einer Exchange 2003-Front-End- und Back-End-Serverarchitektur müssen Sie die formularbasierte Authentifizierung auf dem Front-End-Server aktivieren.

Mit der formularbasierten Authentifizierung kann ein Administrator Benutzer abmelden, wenn diese eine Zeit lang inaktiv sind. Exchange Server 2003 verwendet die folgenden Informationen, um die Aktivität von Benutzern zu ermitteln

- Interaktion zwischen Client und Server wird als aktiv betrachtet. Wenn ein Benutzer beispielsweise ein Objekt öffnet oder sendet, Ordner oder Module wechselt bzw. die Ansicht oder das Webbrowserfenster aktualisiert, wird dies als Aktivität angesehen.
- Wenn ein Benutzer Text in Outlook Web Access-Objekte eingibt, wird dies nicht als Aktivität gewertet. Wenn ein Benutzer zum Beispiel Termine, Besprechungsanforderungen, Bereitstellungen, Ansprechpartner, Aufgaben oder andere Informationen eingibt, ist er nicht aktiv.

Hinweis:

Die Premiumversion von Outlook Web Access hat einen speziellen Code, so dass die Eingabe von Nachrichtentext als Aktivität betrachtet wird.

Wichtig:

Aktivieren Sie SSL (Secure Sockets Layer) auf dem Server, bevor Sie die formularbasierte Authentifizierung aktivieren.

Wichtig:

Bei der formularbasierten Authentifizierung in Exchange Server 2003 darf die Standarddomäneneinstellung in ISS nicht verändert werden. Verwenden Sie daher ausschließlich die Standardeinstellung \. Diese Beschränkung dient der Unterstützung von Benutzeranmeldungen, bei denen das UPN (Unified Principal Name)-Format verwendet wird. Wenn die Standardomäneneinstellung geändert wird, setzt Exchange-System-Manager die Standarddomäneneinstellung auf dem Server auf "\". Sie können dieses Verfahren ändern, indem Sie die Logon.asp-Seite im virtuellen Outlook Web Access-Verzeichnis in IIS anpassen, um Ihre Domäne anzugeben oder eine Liste mit Domänennamen einzubeziehen.

Hinweis:

Wenn Sie die Logon.asp-Seite im virtuellen Outlook Web Access-Verzeichnis in IIS anpassen, werden Ihre Änderungen beim Aktualisieren oder beim erneuten Installieren von Exchange Server 2003 möglicherweise überschrieben.

Ausführliche Anweisungen zur Konfiguration der formularbasierten Authentifizierung finden Sie unter Konfigurieren der formularbasierten Authentifizierung in Exchange Server 2003.

Konfigurieren eines Front-End-Servers als Standarddomäne

Sie können einen Front-End-Server als Standarddomäne konfigurieren, damit sich Benutzer ihre Domäne nicht merken müssen.

Bevor Sie beginnen

Bevor Sie die Verfahren in diesem Thema ausführen, ist es wichtig, dass Sie zunächst den Abschnitt Konfigurieren von Exchange-Front-End-Servern lesen.

Verfahren

So konfigurieren Sie einen Front-End-Server als Standarddomäne

1. Starten Sie **Exchange-System-Manager**auf dem Front-End-Server. Klicken Sie auf **Start**, zeigen Sie auf **Programme**, zeigen Sie auf **Microsoft Exchange**, und klicken Sie dann auf **System-Manager**.
2. Klicken Sie mit der rechten Maustaste auf das virtuelle Exchange-Verzeichnis, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Zugriff**, und klicken Sie dann auf

Authentifizierung.

4. Aktivieren Sie das Kontrollkästchen **Standardauthentifizierung**, und geben Sie dann den Domänennamen im Feld **Standarddomäne** ein.
5. Wiederholen Sie dieses Verfahren für das virtuelle Verzeichnis "Öffentlich".

Hinweis:

Stellen Sie sicher, dass der Systemaufsichtsdienst ausgeführt wird, so dass die Konfigurationseinstellungen vom Verzeichnis in die IIS-Metabasis repliziert werden (Sie können ebenfalls den Systemaufsichtsdienst erneut starten, um die Replikation zu erzwingen).

Konfigurieren der formularbasierten Authentifizierung in Exchange Server 2003

Für Microsoft® Exchange Server 2003 können Sie die neue Funktion zur formularbasierten Authentifizierung für Ihre Microsoft Office Outlook® Web Access-Clients aktivieren. Mit der formularbasierten Authentifizierung kann ein Administrator Benutzer abmelden, wenn diese eine Zeit lang inaktiv sind.

Bevor Sie beginnen

Zum erfolgreichen Durchführen der Verfahren dieses Themas müssen folgende Voraussetzungen erfüllt sein:

- SSL (Secure Sockets Layer) ist auf dem Front-End-Server aktiviert.

Verfahren

So konfigurieren Sie die formularbasierte Authentifizierung in Exchange Server 2003

1. Erweitern Sie im Exchange-System-Manager **Administrative Gruppen**, falls diese aktiviert sind, erweitern Sie **Server** und dann den Front-End-Server, auf dem die formularbasierte Authentifizierung aktiviert werden soll.
2. Erweitern Sie **Protokolle** und **HTTP**, klicken Sie mit der rechten Maustaste auf **Virtueller Exchange-Server**, und wählen Sie dann **Eigenschaften** aus.
3. Wählen Sie die Registerkarte **Einstellungen** aus, und aktivieren Sie dann das Kontrollkästchen **Formularbasierte Authentifizierung aktivieren**.
4. Wählen Sie im Dropdown-Menü neben **Komprimierung** den Komprimierungsgrad

aus (**Hoch**, **Niedrig** oder **Keine**).

Hinweis:

Die Aktivierung der Komprimierung in einer Umgebung mit einem einzelnen Server wird nicht empfohlen. Bei Aktivierung der Komprimierung in einer Umgebung mit einem einzelnen Server wird der Server zusätzlich belastet.

5. Klicken Sie auf **OK**.
6. Wenn Sie eine Meldung erhalten, dass der IIS-Dienst neu gestartet werden muss, klicken Sie auf **OK**, und Starten Sie Microsoft Internet Information Services (IIS) neu.

Zulassen einer E-Mail-Adresse als Anmeldebenutzername

Eine weitere Authentifizierungoption ist die Konfiguration eines Benutzerprinzipalnamens (User Principal Name, UPN) für Benutzer. Mit dieser Option können Benutzer ihre E-Mail-Adresse als ihren Benutzernamen eingeben. Sie müssen alle virtuellen Server und Verzeichnisse auf allen Front-End- und Back-End-Servern konfigurieren, auf die mit UPN-Authentifizierung zugegriffen wird. Nach der Konfiguration eines UPN in den Eigenschaften der virtuellen Server und Verzeichnisse auf allen Front-End- und Back-End-Servern können Benutzer mit dem Benutzernamen *Benutzer@Domäne*.com die Authentifizierung durchführen. Benutzer können sich jedoch weiterhin mit *Domäne\Benutzername* anmelden.

Ausführliche Anweisungen zum Verwenden einer E-Mail-Adresse als Anmeldebenutzername finden Sie unter Zulassen einer E-Mail-Adresse als Anmeldebenutzername.

Zulassen einer E-Mail-Adresse als Anmeldebenutzername

Sie können Exchange Server 2003 so konfigurieren, dass Benutzer ihre E-Mail-Adresse als Anmeldebenutzername verwenden können. Dieses Verfahren wird auch als Konfiguration eines Benutzerprinzipalnamens (UPN, User Principal Name) für Benutzer bezeichnet. Nach der Konfiguration eines UPN auf einem virtuellen Server, auf den der Zugriff für die UPN-Authentifizierung erfolgt, können sich Benutzer mit user@example.com als ihr Benutzername authentifizieren.

Bevor Sie beginnen

Berücksichtigen Sie vor dem Ausführen der Verfahren in diesem Thema die folgenden Aspekte:

- Dieser Vorgang muss auf allen virtuellen Servern und virtuellen Verzeichnissen auf allen Front-End- und Back-End-Servern durchgeführt werden, auf die Benutzer anhand der UPN-Authentifizierung zugreifen.

Verfahren

So lassen Sie eine E-Mail-Adresse als Anmeldebenutzername zu

1. Klicken Sie auf **Start**, zeigen Sie auf **Programme**, zeigen Sie auf **Microsoft Exchange**, und klicken Sie dann auf **System-Manager**.
2. Wenn administrative Gruppen im Exchange-System-Manager angezeigt werden, erweitern Sie **Administrative Gruppen**, erweitern Sie **Server**, und erweitern Sie anschließend den Server, für den Sie die Verwendung einer E-Mail-Adresse als Anmeldename des Benutzers konfigurieren möchten.
3. Erweitern Sie **Protokolle**, **HTTP** und das virtuelle Verzeichnis, das Sie konfigurieren möchten. Wählen Sie anschließend **Eigenschaften** aus.
4. Wählen Sie die Registerkarte **Zugriff** aus, und klicken Sie dann auf **Authentifizierung**.
5. Geben Sie im Feld **Standarddomäne** eine Schrägstrich ein (\).

Deaktivieren von nicht mehr benötigten Diensten

Auf einem Front-End-Server werden nicht alle Exchange-Dienste benötigt. Ihr Einsatz richtet sich nach den jeweils bereitgestellten Protokollen und danach, ob nach dem ursprünglichen Setup Änderungen an der Konfiguration vorgenommen werden. Verwenden Sie zum Beenden und Deaktivieren der Dienste das Snap-In **Dienste** in der Microsoft Management Console. In der folgenden Tabelle werden alle erforderlichen Exchange-Dienste aufgelistet. Beenden und deaktivieren Sie alle anderen Exchange-Dienste.

Für den Clientzugriff erforderliche Exchange-Dienste

Clientzugriffsmethode	Erforderliche Dienste	Beschreibung
HTTP (Outlook Web Access, WebDAV, Exchange ActiveSync®)	WWW-Publishingdienst (W3SVC)	Die Exchange-Systemaufsicht sollte ebenfalls aktiviert sein. Ermöglicht Verwaltung und IIS-Metabaseaktualisierung
POP3	Microsoft Exchange POP3 (POP3Svc)	Die Exchange-Systemaufsicht sollte ebenfalls aktiviert sein. Ermöglicht Verwaltung und IIS-Metabaseaktualisierung
IMAP4	Microsoft Exchange IMAP4 (IMAP4Svc)	Die Exchange-Systemaufsicht sollte ebenfalls aktiviert sein. Ermöglicht Verwaltung und IIS-Metabaseaktualisierung
SMTP	SMTP-Protokoll (SMTPSVC), Microsoft Exchange-Systemaufsicht (MSExchangeSA), Microsoft Exchange-Informationsspeicher (MSExchangeIS)	SMTP verwendet den Exchange-Informationsspeicher zur DNS-Formatierung. Wenn ein Server SMTP ausführt, sollte er ebenfalls den Microsoft Exchange-Routingdienst (RESVC) ausführen.

Grundsätzlich sollte die Systemaufsicht auf einem Front-End-Server ausgeführt werden. Auch wenn dies für einige Protokolle nicht erforderlich ist, treten bestimmte Tasks nur auf, wenn die Systemaufsicht ausgeführt wird. Weiterhin sind zusätzliche Dienste je nach den vom Front-End-Server ausgeführten Funktionen erforderlich. Wenn der Server beispielsweise WMI-Automation ausführt, muss der Exchange-Verwaltungsdienst ausgeführt werden.

Hinweis:

Bei einer Aktualisierung muss NNTP auf dem Server aktiviert sein. Dieser Dienst kann jedoch auch deaktiviert werden, wenn Sie Ihren Benutzer NNTP nicht bereitstellen.

URLSCan und IIS Lockdown-Assistent

Vor dem Einsatz von Servern im Internet müssen Sie IIS sichern, indem Sie alle nicht benötigten Features und Dienste deaktivieren. In Windows 2003 Server sind viele vom Server nicht benötigten IIS-Features bereits deaktiviert. Laden Sie unter Microsoft Windows 2000 Server, den IIS Lockdown-Assistenten herunter, und führen Sie ihn aus.

Informationen zum Installieren und Verwenden des IIS Lockdown-Assistenten finden Sie im Microsoft Knowledge Base-Artikel 325864, "Installieren und Verwenden des IIS-Lockdown-Assistenten."

Das IIS Lockdown-Tool (Version 2.1) erhalten Sie unter http://go.microsoft.com/fwlink/?linkid=12281.

Hinweis:

Führen Sie zur Maximierung der Sicherheit Ihrer Exchange-Server vor und nach der Verwendung des IIS Lockdown-Assistenten alle erforderlichen Aktualisierungen aus. Mögliche Sicherheitslücken in Exchange Server können durch regelmäßige Aktualisierungen geschlossen werden.

Mit dem IIS Lockdown-Assistenten können Sie nicht mehr benötigte IIS 5.0-Features und -Dienste je nach ausgeführter Serversoftware deaktivieren. Zur Bereitstellung mehrerer Sicherheitsebenen gegen Angreifer enthält der IIS Lockdown-Assistent ebenfalls URLScan. Dieses Tool analysiert HTTP-Anfragen, die IIS empfängt und bei Verdacht ablehnt.

IIS Lockdown-Assistent enthält ebenfalls eine Konfigurationsvorlage für Exchange, die nicht gewünschte Features und Dienste deaktiviert. Führen Sie zur Verwendung dieser Konfigurationsvorlage den IIS Lockdown-Assistenten aus, wählen Sie die Exchange-Vorlagen, und ändern Sie dann die Standardkonfigurationsoptionen, oder akzeptieren Sie sie.

Laden Sie URLScan separat herunter, wenn Sie das Tool unter Windows Server 2003 ausführen möchten. Eine Liste der neben den in IIS 6.0 verfügbaren URLScan-Features erhalten Sie unter http://go.microsoft.com/fwlink/?linkid=24490.

URLScan wird in folgendem Ordner installiert: ***<Laufwerk:>*/*<Windows-Verzeichnis>*/system32/inetsrv/urlscan**.

Eine ordnungsgemäße Konfiguration von URLScan ist zur Verwendung in Exchange Server erforderlich. Umfassende Informationen zum Konfigurieren von URLScan zur Verwendung mit Exchange Server finden Sie in den folgenden Microsoft Knowledge Base-Artikeln:

- Informationen zu Exchange Server 2000 enthält Artikel 309677 der Microsoft Knowledge Base, "Known issues and fine tuning when you use the IIS Lockdown Wizard in an Exchange 2000 Server environment".

- Exchange Server 2003 - Microsoft Knowledge Base-Artikel 823175, "Bekannte Probleme und die feine Optimierung, wenn Sie das URLScan-Dienstprogramm in einer Umgebung von Exchange 2003 verwenden."

Der Abschnitt enthält weiterhin Informationen darüber, warum einige URLScan-Einstellungen erforderlich sind. Wenn Sie nach dem Ausführen des Assistenten die folgenden Einstellungen in der Datei **UrlScan.ini** nicht konfigurieren, werden einige Outlook Web Access-Features möglicherweise nicht ordnungsgemäß ausgeführt:

- **Allow Dot In Path** Stellen Sie sicher, dass diese Einstellung auf "1" gesetzt ist, so dass der Zugriff auf Outlook Web Access-Anhänge möglich ist frühere Browser-Versionen Outlook Web Access verwenden können.
- **File Extensions** HTR-Dateien sind standardmäßig deaktiviert. Bei Deaktivierung dieses Dateityps kann das Feature zum Ändern des Kennworts in Outlook Web Access nicht ausgeführt werden.
- **Deny Url Sequences** Im Abschnitt [DenyUrlSequences] wirken sich explizit geblockte Sequenzen möglicherweise auf den Outlook Web Access-Zugriff aus. Der Zugriff wird verweigert, wenn in der Betreffzeile einer E-Mail oder im Namen eines E-Mail-Ordners die folgenden Zeichen enthalten sind:
  - Punkt (.)
  - Doppelpunkt (..)
  - Punkt und Schrägstrich (./)
  - Umgekehrter Schrägstrich (\)
  - Prozentzeichen (%)
  - Kaufmännisches Und (&)

Treten weitere Probleme bei der Verarbeitung von Outlook Web Access-Anfragen mit aktiviertem URLScan auf, überprüfen Sie in der URLScan-Protokolldatei (UrlScan.log) die Liste der Anfragen, die abgelehnt wurden.

Trennen und Löschen von Öffentlichen Informationsspeichern und Postfachspeichern

Wenn Sie SMTP auf dem Front-End-Server nicht verwenden, trennen Sie die Verbindung zu den Öffentlichen Informationsspeichern, und löschen Sie sie. Wenn Sie SMTP auf dem Front-End-Server verwenden, benötigen Sie einen Postfachspeicher, da der SMTP-Dienst einen bereitgestellten Postfachspeicher zur Durchführung von Konvertierungen benötigt. Dieser bereitgestellte Postfachspeicher sollte jedoch keine Postfächer enthalten. Ein

Öffentlicher Informationsspeicher sollte nie auf dem Front-End-Server bereitgestellt werden. Weitere Informationen finden Sie unter Ausführen von SMTP für POP- und IMAP-Clients.

Der Microsoft Exchange-Informationsspeicherdienst (MSExchangeIS) kann nur gestartet werden, wenn mindestens eine Speichergruppe festgelegt ist. Wenn der MSExchangeIS-Dienst ausgeführt werden muss, löschen Sie nach dem Löschen der Öffentlichen und Privaten Informationsspeichern nicht die Speichergruppe auf dem Front-End-Server.

Hinweis:

Wird der MSExchangeIS-Dienst in Exchange 2000 Server nicht ausgeführt, können Sie mit dem Internetdienste-Manager keine Konfigurationsänderungen vornehmen. Wenn Sie die Konfiguration mit dem Internetdienste-Manager ändern müssen (z. B. zur Konfiguration der SSL-Verschlüsselung), stellen Sie sicher, dass Sie diese Schritte vor dem Löschen der Postfachspeicher und der Informationsspeicher für Öffentliche Ordner ausführen. Dieses Verfahren gilt nicht mehr für Exchange Server 2003.

Konfigurieren von Netzwerklastenausgleich

Möglicherweise möchten Sie die Datenlast auf Ihre Front-End-Server verteilen. Verwenden Sie hierfür nicht die Windows Clustering Services, da auf den Front-End-Servern keine Daten gespeichert werden. Jeder Front-End-Server ist im Wesentlichen eine Kopie des anderen, so dass ein Failover nicht sinnvoll ist. Verwenden Sie den Netzwerklastenausgleich, um die Clientanfragen gleichmäßig auf mehrere Front-End-Server zu verteilen. Weitere Informationen hierzu finden Sie unter Netzwerklastenausgleich-Cluster.

Konfigurieren von SSL (Secure Sockets Layer)

Die Schritte für die Konfiguration von SSL für POP, IMAP und SMTP weichen von denjenigen für HTTP ab.

- Ausführliche Anweisungen zum Konfigurieren von SSL für POP3, IMAP4 und SMTP finden Sie unter Konfigurieren von SSL für POP3, IMAP4 und SMTP.
- Ausführliche Anweisungen zum Konfigurieren von SSL für HTTP finden Sie unter Konfigurieren von SSL für HTTP.

Konfigurieren von SSL für POP3, IMAP4 und SMTP

Sie können virtuelle Server unter Exchange Server zur Verwendung von SSL (Secure Sockets Layer) konfigurieren.

Verfahren

So konfigurieren Sie SSL für POP3, IMAP4 und SMTP

1. Klicken Sie mit der rechten Maustaste im Exchange-System-Manager auf den virtuellen Server, und klicken Sie anschließend auf **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Zugriff**, und klicken Sie anschließend auf **Certificate**.
3. Folgend Sie den Anweisungen im Assistenten unter Verwendung der Richtlinien in der Onlinehilfe, um das SSL-Zertifikat anzufordern und zu installieren.

Konfigurieren von SSL für HTTP

Sie können einen virtuellen HTTP-Server von Exchange für die Verwendung von SSL konfigurieren.

Verfahren

So konfigurieren Sie SSL für HTTP

1. Klicken Sie für den virtuellen HTTP-Standardserver von Exchange im Internetdienste-Manager auf **Standardwebsite**, und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Verzeichnissicherheit**, und wählen Sie dann **Serverzertifikat** aus.
3. Folgen Sie den Anweisungen des Assistenten, und verwenden Sie die Produktdokumentation zu Internet Information Services 6.0 als Referenz, um das SSL-Zertifikat anzufordern und zu installieren. HTTP SSL wird für jeden virtuellen Server oder für jede Website separat konfiguriert, so dass Sie beim Erstellen von zusätzlichen virtuellen HTTP-Servern im Exchange-System-Manager SSL für jeden

Server oder jede Website wie im Internetdienste-Manager vorgegeben konfigurieren müssen.

Weitere Informationen

Weitere Informationen zur Verwendung von Internet Information Services 6.0 finden Sie unter Produktdokumentation zu Internet Information Services 6.0.

Konfigurieren von SMTP auf dem Front-End-Server

SMTP muss auf dem Front-End-Server verfügbar sein, damit POP- und IMAP-Clients E-Mail-Nachrichten weiterleiten können. Sie können SMTP auf einem Front-End-Server installieren oder einen separaten SMTP-Server einrichten. Konfigurieren Sie zum Installieren von SMTP auf dem Front-End-Server SMTP für interne und externe Domänen. Dieses Verfahren wird in den folgenden beiden Abschnitten erläutert.

E-Mail für interne Domänen

Damit der Front-End-Server E-Mail-Nachrichten aus dem Internet akzeptiert, muss der Front-End-Server die Domäne kennen, für die er die E-Mail-Nachrichten akzeptieren soll. Durch das Hinzufügen von Empfängerrichtlinien für alle Domänen wird der Server in der Exchange-Organisation angewiesen, E-Mail-Nachrichten für solche Domänen zu akzeptieren. Weiterhin müssen Sie den anonymen Zugriff für andere SMTP-Server im Internet aktivieren, um E-Mail erfolgreich an Ihre Organisation weiterzuleiten (dies ist die Standardeinstellung).

E-Mail für externe Domänen

In der Standardkonfiguration werden alle an Ihren Server weitergeleiteten und an externe Domänen adressierte SMTP-E-Mail-Nachrichten verweigert. Dies liegt daran, dass die Weiterleitung für den gesamten anonymen Zugriff deaktiviert ist (authentifizierte Benutzer können jedoch nach wie vor E-Mail-Nachrichten an beliebige externe Domänen senden). Benutzer, die eine E-Mail anonym an externe Domänen weiterleiten möchten, erhalten eine Fehlermeldung, wie zum Beispiel "550 5.7.1 Nachricht für suzan@adatum.com kann nicht weitergeleitet werden". Die Clients müssen zur Verwendung der SMTP-Authentifizierung konfiguriert werden.

Hinweis:

Obwohl die Weiterleitung bei anonymem Zugriff aktiviert werden kann, wird diese Methode nicht empfohlen und sollte nicht notwendig sein. Bei der Weiterleitung bei

anonymem Zugriff kann jeder Benutzer über das Internet Ihren Server zum Senden von E-Mail-Nachrichten verwenden.

Wenn Sie die SMTP-Authentifizierung für E-Mail-Nachrichten von Benutzern aus dem Internet verwenden möchten, sollten Sie ebenfalls SSL für Klartext oder Standardauthentifizierung auswählen, um firmeninterne Benutzernamen und Kennwörter nicht unverschlüsselt zu senden. Konfigurieren von SSL für die Standardauthentifizierung in den **Eigenschaften** des virtuellen SMTP-Servers: Klicken Sie auf der Registerkarte **Zugriff** auf **Authentifizierung**, und wählen Sie dann **TLS-Verschlüsselung erforderlich**.

Weitere Informationen zu SMTP finden Sie im Transport- und Routing-Handbuch für Exchange Server 2003.

Konfigurieren von DSAccess für Perimeternetzwerke

Die DSAccess-Komponente in Exchange 2000ServerSP2 wurde überarbeitet, um den Support für Umkreisnetzwerke zu verbessern, in denen RPC-Datenverkehr über die Internetfirewall nicht erlaubt ist. Zur Vermeidung von Leistungsproblemen werden jedoch zwei zusätzliche Registrierungsschlüssel bereitgestellt, die auf dem Front-End-Server festgelegt werden sollten, um NetLogon und die Ping-Funktion des Verzeichniszugriffs zu deaktivieren. Weiterhin können Sie DSAccess so konfigurieren, dass Ihre Front-End-Server bestimmte Domänencontroller und globale Katalogserver kontaktieren. In den folgenden Abschnitten wird die Konfiguration dieser Einstellungen erläutert.

Hinweis:

Dieser Abschnitt enthält Informationen zum Bearbeiten der Registrierung. Die fehlerhafte Bearbeitung der Registrierung kann zu ernsthaften Problemen führen, die möglicherweise eine Neuinstallation des Betriebssystems erforderlich machen. Dadurch entstandene Probleme können unter Umständen nicht mehr behoben werden. Sichern Sie vor dem Ändern der Registrierung alle wichtigen Daten.

Hinweis:

Die fehlerhafte Verwendung des Registrierungs-Editors kann zu ernsthaften Problemen führen, die möglicherweise eine Neuinstallation des Betriebssystems erforderlich machen. Microsoft übernimmt keine Garantie dafür, dass durch unsachgemäßes Verwenden des Registrierungs-Editors verursachte Probleme behoben werden können. Sie verwenden den Registrierungs-Editor auf eigene Verantwortung. Informationen zum Bearbeiten der Registrierung finden Sie unter "Ändern von Schlüsseln und Werten" in der Hilfe zum Registrierungs-Editor (Regedit.exe) oder unter "Hinzufügen und Löschen von Daten in der Registrierung" und "Bearbeiten der Registrierungsdaten" in der Hilfe zu Regedt32.exe Beachten

Sie, dass die Registrierung vor der Bearbeitung gesichert werden sollte. Beim Ausführen von Microsoft Windows NT® Server oder Windows 2000 Server sollten Sie Ihre Notfalldiskette ebenfalls aktualisieren.

Deaktivieren NetLogon-Überprüfung

DSAccess stellt eine Verbindung zu Active Directory-Servern her, um den verfügbaren Speicherplatz, die Synchronisierungsdauer sowie die Replikationsteilnahme unter Verwendung des NetLogon-Dienstes mit RPC zu überprüfen. Wenn Sie RPC-Datenverkehr über die interne Firewall nicht zulassen möchten, sollten Sie die NetLogon-Überprüfung beenden, indem Sie den DisableNetlogonCheck-Registrierungsschlüssel auf dem Front-End-Server erstellen.

Ausführliche Anweisungen zur Deaktivierung der NetLogon-Überprüfung finden Sie unter Vorgehensweise beim Deaktivieren der NetLogon-Überprüfung auf einem Front-End-Server.

Deaktivieren der Ping-Funktion des Verzeichniszugriffs

In einem Umkreisnetzwerk müssen Sie ebenfalls einen Registrierungsschlüssel auf dem Front-End-Server erstellen, um Verzeichniszugriffe von pingenden Domänencontrollern zu verhindern.

Ausführliche Anweisungen zur Deaktivierung des Verzeichniszugriffs mit der Ping-Funktion finden Sie unter Deaktivieren der Pingausführung durch den Verzeichniszugriff.

Festlegen von Domänencontrollern und globalen Katalogservern

In einem Umkreisnetzwerk möchten Sie ggf. DSAccess zur Verwendung von bestimmten Domänencontrollern und globalen Katalogservern konfigurieren und anschließend IP-Filter einsetzen, um sicherzustellen, dass die Front-End-Server nur Verbindungen zu diesen Domänencontrollern und globalen Katalogservern herstellen. Verwenden Sie zum Festlegen von Domänencontrollern und globalen Katalogservern die Registerkarte **Verzeichniszugriff** im Dialogfeld ***<Servername>* Eigenschaften**. Durch die Angabe von Servern auf der Registerkarte **Verzeichniszugriff** werden Schlüssel in der Registrierung gesetzt. In früheren Exchange-Versionen war die Registerkarte **Verzeichniszugriff** nicht verfügbar. Zu einem früheren Zeitpunkt zur Angabe von Domänencontrollern und globalen Katalogservern festgelegte Registrierungsschlüssel können immer noch eingesetzt werden.

Vorgehensweise beim Deaktivieren der NetLogon-Überprüfung auf einem Front-End-Server

DSAccess stellt eine Verbindung zu Active Directory-Servern her, um den verfügbaren Speicherplatz, die Synchronisierungsdauer sowie die Replikationsteilnahme unter Verwendung des NetLogon-Dienstes mit RPC zu überprüfen. In diesem Verfahren wird die Deaktivierung der NetLogon-Überprüfung erläutert.

Bevor Sie beginnen

Dieses Thema enthält Informationen zum Bearbeiten der Registrierung.

Vorsicht:

Die fehlerhafte Bearbeitung der Registrierung kann zu ernsthaften Problemen führen, die möglicherweise eine Neuinstallation des Betriebssystems erforderlich machen. Dadurch entstandene Probleme können unter Umständen nicht mehr behoben werden. Sichern Sie vor dem Ändern der Registrierung alle wichtigen Daten.

Verfahren

So deaktivieren Sie die NetLogon-Überprüfung

1. Starten Sie den Registrierungs-Editor (regedit).
2. Navigieren Sie in der Registrierung zu folgendem Schlüssel: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess\
3. Klicken Sie im Menü **Bearbeiten** auf **Wert hinzufügen**, und fügen Sie dann folgenden Registrierungsschlüssel hinzu:

   Name des Werts: DisableNetlogonCheck

   Datentyp: REG_DWORD

   Daten für Wert: 1

Deaktivieren der Pingausführung durch den Verzeichniszugriff

In diesem Verfahren wird beschrieben, wie das Pingen von Domänencontrollern durch DSAccess deaktiviert wird.

Bevor Sie beginnen

Dieses Thema enthält Informationen zum Bearbeiten der Registrierung.

Vorsicht:

Die fehlerhafte Bearbeitung der Registrierung kann zu ernsthaften Problemen führen, die möglicherweise eine Neuinstallation des Betriebssystems erforderlich machen. Dadurch entstandene Probleme können unter Umständen nicht mehr behoben werden. Sichern Sie vor dem Ändern der Registrierung alle wichtigen Daten.

Verfahren

So deaktivieren Sie die Ausführung des Ping-Befehls durch den Verzeichnisdienst

1. Starten Sie den Registrierungs-Editor (Regedit.exe).
2. Navigieren Sie in der Registrierung zu folgendem Schlüssel: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess\
3. Klicken Sie im Menü **Bearbeiten** auf **Wert hinzufügen**, und fügen Sie dann folgenden Registrierungsschlüssel hinzu:

   Name des Werts: LdapKeepAliveSecs

   Datentyp: REG_DWORD

   Daten für Wert: 0

Hosten von mehreren Domänen

In der einfachsten Topologie müssen Sie den Front-End-Server nicht konfigurieren, sondern lediglich als einen Front-End-Server festlegen. Wenn Sie jedoch mehrere Domänen,

Organisationen oder Öffentliche Ordner-Strukturen hosten, ist das Erstellen von zusätzlichen virtuellen Servern oder Verzeichnissen unter Umständen erforderlich.

Vor Exchange Server 2003 SP1 war für jede zu hostende Domäne ein eindeutiger virtueller Server oder ein virtuelles Verzeichnis erforderlich, damit Benutzer mit E-Mail-Adressen von diesen Domänen sich am jeweiligen virtuellen Server oder Verzeichnis anmelden konnten. Wenn Sie weitere Domänen hosten, stehen zwei Methoden zur Konfiguration des virtuellen HTTP-Servers zur Verfügung:

- Methode eins: Erstellen zusätzlicher virtueller Server
- Methode zwei: Erstellen zusätzlicher virtueller Verzeichnisse

In der folgenden Methode ist Ihre Exchange-Standarddomäne microsoft.com, und Sie hosten Postfächer für adatum.com und Öffentliche Ordner für contoso.com. Die Methoden erläutern die Konfiguration Ihrer Front-End- und Back-End-Server für diese gehosteten Unternehmen.

Hinweis:

In Exchange Server 2003 Service Pack 1 müssen Sie jetzt keine zusätzlichen virtuellen Server und virtuellen Verzeichnisse für verschiedene SMTP-Domänen mehr erstellen. Die Verwendung von mehreren virtuellen Verzeichnissen und virtuellen Servern hat jedoch weiterhin logistische bzw. ästhetische Gründe. Weitere Informationen zur Outlook Web Access-Anmelde- und SMTP-Domäne finden Sie unter "Anmelden an Outlook Web Access" in Unterstützung für HTTP-Zugriff.

Methode eins: Erstellen zusätzlicher virtueller Server

Bei dieser Methode erstellen Sie einen virtuellen Server für jede zu hostende Domäne. Sie verfügen beispielsweise über drei virtuelle HTTP-Server auf jedem Server unter Exchange: einer ist der virtuelle Exchange-Standardserver, einer der virtuelle Server für die Postfächer von adatum.com und einer der virtuelle Server für die Öffentliche Ordner-Struktur von contoso.com. Diese Methode bietet ein Höchstmaß an Flexibilität beim festlegen der für jede Domäne verfügbaren Ressourcen.

Jeder virtuelle HTTP-Server muss über eine eindeutige Kombination aus IP-Adresse, Hostheader und Anschluss verfügen. Der Hostheader ist der DNS-Name Ihrer Website. Wenn Benutzer beispielsweise auf Ihre Website anhand der Eingabe von http://www.contoso.com/example in einem Browser zugreifen, handelt es sich bei dem Hostheader um www.contoso.com. Wenn Sie den Hostheader für den virtuellen Server angeben, können Sie mehrere Websites mit derselben Kombination aus Anschluss und IP-Adresse verwenden, da der Hostheader Eindeutigkeit gewährleistet. Wenn Sie jedoch versuchen, einen virtuellen Server mit denselben Einstellungen eines anderen Servers zu erstellen, kann der neue virtuelle Server nicht gestartet werden.

Wenn zusätzliche virtuelle Server eingerichtet werden und die Sitzungen nicht verschlüsselt sind, werden Clientanfragen wir folgt an den richtigen virtuellen Server geleitet:

1. Der Client stellt eine Verbindung zum Front-End-Server her.
2. Der Server empfängt ein Paket mit der IP-Adresse, dem angeforderten Anschluss und dem Hostheader.
3. Der Server verwendet diese Informationen, um den jeweiligen virtuellen Server zu suchen, der die Anfrage verarbeiten soll.

Wenn die Anfrage eines Benutzers an den richtigen virtuellen Server geleitet wird, kann nicht garantiert werden, dass der Benutzer erfolgreich auf Outlook Web Access zugreifen kann. Für die Anmeldung an den virtuellen Server muss der Benutzer ebenfalls über eine E-Mail-Adresse der SMTP-Domäne verfügen, die mit dem virtuellen Server verknüpft ist. Alle virtuellen Server und Verzeichnisse, die auf Postfächer verweisen, sind mit einer bestimmten SMTP-Domäne verknüpft. Beim Erstellen von zusätzlichen virtuellen Servern, die auf Postfächer verweisen, müssen Sie den virtuellen Server mit der jeweiligen Domäne verknüpfen. (Beim Einrichten von Exchange wird die virtuelle Exchange-HTTP-Standarddomäne mit der Exchange-Standarddomäne verknüpft. Diese Standardeinstellung kann nicht geändert werden.)

Nachdem die Anfrage des Benutzers and den richtigen virtuellen Server weitergeleitet wurde, wird der Prozess wie folgt fortgeführt:

1. Der virtuelle Server verwendet die Authentifizierungsinformationen des Benutzers, um ihn in Active Directory zu suchen.
2. Wenn der Benutzer eine E-Mail-Adresse aus der mit diesem virtuellen Server verknüpften SMTP-Domäne hat, erteilt der virtuelle Server den Zugriff. Andernfalls wird der Zugriff vom virtuellen Server verweigert.

   Hinweis:

   Authentifizierungsinformationen können nur dann für die Suche der SMTP-Proxyadresse des Benutzers verwendet werden, wenn die Authentifizierung auf dem Front-End-Server aktiviert ist. Ist die Authentifizierung nicht aktiviert, verwendet der Server den im URL angegebenen Alias (da sich der Benutzer für den Zugriff auf Outlook Web Access über einen Front-End-Server mit Pass-Through-Authentifizierung explizit im Format http://server/exchange/user anmelden muss). Zur Bildung der Proxyadresse kombiniert der Server anschließend den Alias mit der SMTP-Domäne in den Eigenschaften des virtuellen Servers.

Hinweis:

Bei Verwendung von SSL ist der Hostheader im verschlüsselten Teil des Pakets enthalten. Im nicht verschlüsselten Teil sind lediglich die IP-Adresse und der Anschluss verfügbar. Um festzulegen, welches SSL-Zertifikat zum Entschlüsseln der

Daten verwendet werden soll, muss der Server in der Lage sein, den jeweiligen virtuellen Server mit einer eindeutigen Kombination aus IP-Adresse und Anschluss anzugeben. Bei Verwendung von SSL (wenn z. B. der Front-End-Server im Internet bereitgestellt wird) muss die IP-Adresse gesondert mit dem jeweiligen virtuellen Server verknüpft werden.

Nachdem Sie den zusätzlichen virtuellen Server erstellt haben, müssen Sie die virtuellen Exchange-Verzeichnisse und öffentlichen Verzeichnisse unter diesem virtuellen Server erstellen.

Anweisungen zum Erstellen von virtuellen Verzeichnissen finden Sie unter Hinzufügen eines virtuellen Verzeichnisses auf einem virtuellen HTTP-Server in Exchange Server 2003.

Hinweis:

Wenn Sie das Feature zum Ändern des Kennworts für Ihre Benutzer aktivieren möchten, müssen Sie es für alle virtuellen Server auf dem Front-End-Server aktivieren. Alle virtuellen Server müssen das virtuelle Verzeichnis **IISAdmPwd** enthalten.

Methode zwei: Erstellen zusätzlicher virtueller Verzeichnisse

Die zweite Methode zum Konfigurieren von mehreren gehosteten Domänen besteht darin, jeder Domäne ein virtuelles Verzeichnis hinzuzufügen. Für den Zugriff auf Postfachspeicher müssen Sie die Domäne in den Eigenschaften des virtuellen Verzeichnisses angeben. Für den Zugriff auf Informationsspeicher für Öffentliche Ordner müssen Sie das Stammverzeichnis für Öffentliche Ordner angeben. Fügen Sie dem ersten gehosteten Unternehmen adatum.com ein virtuelles Verzeichnis unter dem virtuellen Exchange-HTTP-Standardserver hinzu. Verwenden Sie einen Namen, der das Unternehmen eindeutig angibt, zum Beispiel Adatum. Klicken Sie in den Eigenschaften des virtuellen Verzeichnisses auf **Ändern**, und wählen Sie dann, wie beim virtuellen Server, adatum.com als SMTP-Domäne aus. Benutzer von adatum.com können sich jetzt mit http://mail.microsoft.com/adatum/ verbinden, um auf ihre Postfächer zuzugreifen.

Fügen Sie ein weiteres virtuelles Verzeichnis für Contoso hinzu, und wählen Sie jetzt **Öffentlicher Ordner**, und geben Sie das Stammverzeichnis für den Öffentlichen Ordner für Contoso an. Benutzer von contoso.com können sich jetzt mit http://mail.microsoft.com/contoso/ verbinden, um auf ihre Öffentlichen Ordner zuzugreifen.

Der Hauptvorteil dieser Methode besteht in der Verwendung von SSL. SSL-Zertifikate werden für einen bestimmten Host- oder Domänennamen ausgegeben, in diesem Fall für mail.microsoft.com. Wenn Sie über mehrere virtuelle Server mit verschiedenen Domänennamen verfügen (zum Beispiel mail.microsoft.com und mail.adatum.com), benötigen Sie ein SSL-Zertifikat für jede Domäne. Dieser Bedarf ist sehr kostenintensiv. Da Clients in Methode zwei über eine einzelne Domäne auf ihre Daten zugreifen

(http://mail.microsoft.com), können Sie die Kosten für zusätzliche Zertifikate einsparen und müssen SSL nicht auf jedem virtuellen Server konfigurieren .

Ausführliche Anweisungen zum Erstellen von neuen virtuellen Verzeichnissen finden Sie unter Erstellen von virtuellen Verzeichnissen.

Wenn Sie mehrere Domänen hosten (wie in der ersten Methode für das Hinzufügen von virtuellen Servern beschrieben) und ein virtueller Server für jede Domäne erstellt wurde, empfehlen wir die Verwendung der Standardnamen für virtuelle Verzeichnisse - "Exchange" für den Postfachzugriff (stellen Sie sicher, dass Sie die Domäne erneut angeben) und "Öffentlich" für den Zugriff auf den Informationsspeicher für Öffentliche Ordner. Erstellen Sie auf keinem zusätzlichen virtuellen Server das virtuelle Verzeichnis "exadmin". Dieses Verzeichnis wird nur vom System-Manager verwendet und wird vom Front-End-Server nicht zwischengespeichert.

Hinzufügen eines virtuellen Verzeichnisses auf einem virtuellen HTTP-Server in Exchange Server 2003

In diesem Thema wird das Hinzufügen eines virtuellen Verzeichnisses auf einem virtuellen HTTP-Server unter Exchange Server 2003 erläutert.

Verfahren

So fügen Sie ein virtuelles Verzeichnis auf einem virtuellen HTTP-Server unter Exchange Server 2003 hinzu

1. Starten Sie den Exchange-System-Manager: Klicken Sie auf **Start**, zeigen Sie auf **Programme**, zeigen Sie auf **Microsoft Exchange**, und klicken Sie dann auf **System-Manager**.
2. Wenn administrative Gruppen im Exchange-System-Manager angezeigt werden, erweitern Sie **Administrative Gruppen**, erweitern Sie **Server**, und erweitern Sie anschließend den Server, für den Sie die Verwendung einer E-Mail-Adresse als Anmeldename des Benutzers konfigurieren möchten.
3. Erweitern Sie **Protokolle** und dann **HTTP**, klicken Sie mit der rechten Maustaste auf den virtuellen HTTP-Server, klicken Sie auf **Neu** und dann auf **Virtuelles Verzeichnis**.
4. Benennen Sie das virtuelle Verzeichnis.

   Notes:

Der verwendete Name ist wichtig, da er vom Client im Browser eingegeben wird (zum Beispiel **http://mail.microsoft.com/***virtuellerverzeichnisname*). Verwenden Sie im Verzeichnisnamen nicht die folgenden Zeichen, da IIS sie blockiert:

- Punkt (.)
- Doppelpunkt (..)
- Punkt und Schrägstrich (./)
- Umgekehrter Schrägstrich (\)
- Prozentzeichen (%)
- Kaufmännisches Und (&)

5. Klicken Sie mit der rechten Maustaste auf das soeben erstellte virtuelle Verzeichnis, und klicken Sie dann auf **Eigenschaften**. Geben Sie an, ob das Verzeichnis für den Zugriff auf einen Postfachspeicher oder einen Speicher für Öffentlich Ordner freigegeben ist. Wenn der Zugriff über das Verzeichnis auf ein Postfachspeicher erfolgen soll, ist die Angabe der SMTP-Domäne erforderlich. Wenn der Zugriff über das virtuelle Verzeichnis auf einen Speicher für Öffentliche Ordner erfolgen soll, wählen Sie den gewünschten Öffentlichen Ordner aus, der als Stammverzeichnis des Öffentlichen Ordners für dieses virtuelle Verzeichnis eingesetzt werden soll.

Weitere Informationen

Weitere Informationen finden Sie unter Konfigurieren von Exchange-Front-End-Servern.

Erstellen von virtuellen Verzeichnissen

Verwenden Sie dieses Verfahren zum Erstellen von virtuellen Verzeichnissen.

Verfahren

So erstellen Sie virtuelle Verzeichnisse

1. Klicken Sie im Exchange-System-Manager mit der rechten Maustaste auf den virtuellen HTTP-Server, klicken Sie auf **Neu** und dann auf **Virtuelles Verzeichnis**.
2. Benennen Sie das virtuelle Verzeichnis.

   Hinweis:

   Der verwendete Name ist wichtig, da er vom Client im Browser eingegeben wird (zum Beispiel **http://mail.microsoft.com/*virtuellerverzeichnisname***).

Verwenden Sie im Verzeichnisnamen nicht die folgenden Zeichen, da IIS sie blockiert:

- Punkt (.)
- Doppelpunkt (..)
- Punkt und Schrägstrich (./)
- Umgekehrter Schrägstrich (\)
- Prozentzeichen (%)
- Kaufmännisches Und (&)

3. Klicken Sie mit der rechten Maustaste auf das soeben erstellte virtuelle Verzeichnis, und klicken Sie dann auf **Eigenschaften**. Geben Sie an, ob das Verzeichnis für den Zugriff auf ein Postfach oder einen Öffentlichen Ordner freigegeben ist. Wenn über das Verzeichnis auf ein Postfachspeicher zugegriffen werden soll, ist die Angabe der SMTP-Domäne erforderlich. Wenn der Zugriff über das virtuelle Verzeichnis auf einen Speicher für Öffentliche Ordner erfolgen soll, wählen Sie den gewünschten Öffentlichen Ordner aus, der als Stammverzeichnis des Öffentlichen Ordners für dieses virtuelle Verzeichnis eingesetzt werden soll.

Konfigurieren eines Back-End-Servers

Die Exchange-Konfiguration ist auf dem Active Directory®-Verzeichnisserver auf einer Gesamtstrukturbasis gespeichert. Dies bedeutet, dass alle Front-End- und Back-End-Server sich in derselben Struktur befinden müssen. Der direkte Zugriff auf Back-End-Server ist möglich, ohne die Front-End- und Back-End-Konfiguration zu beeinträchtigen.

Wenn Sie zusätzliche virtuelle Server oder Verzeichnisse auf einem beliebigen Front-End-Server konfiguriert haben, ist die Konfiguration der Back-End-Server nicht erforderlich. Wenn Sie zusätzliche virtuelle Server und Verzeichnisse auf einem beliebigen Front-End-Server erstellen, müssen Sie jedoch auf den Back-End-Servern übereinstimmende virtuelle Server und Verzeichnisse hinzufügen.

Die jeweiligen Konfigurationsschritte für den Back-End-Server richten sich danach, ob er auf einem Cluster gehostet wird. Die folgenden Schritte beschreiben die Konfiguration für Back-End-Server, die sich nicht in einem Cluster befinden. Weitere Informationen zur Konfiguration von Back-End-Servern in einem Cluster finden Sie in der technischen Dokumentation Bereitstellen von Serverclustern mit Microsoft Exchange 2000.

Hinweis:

Wenn Back-End-Server in einem Cluster bereitgestellt sind, können Sie mit dem Namen des physikalisch gruppierten Computers nicht auf das virtuelle HTTP-Clusterverzeichnis zugreifen. Verwenden Sie den virtuellen Gruppennamen.

Konfigurieren der Authentifizierung auf einem Back-End-Server

Standardmäßig werden virtuelle HTTP-Server auf dem Back-End-Server konfiguriert, um sowohl die Basisauthentifizierung als auch die integrierte Windows-Authentifizierung zu gewährleisten. Die Verwendung dieser Standardkonfiguration wird empfohlen.

Bei der Standardauthentifizierung wird der Benutzername und das Kennwort in einem schwach kodierten (nicht verschlüsselten) Format über das Netzwerk gesendet. Die integrierte Windows-Authentifizierung bezieht sich auf ein Paket von Authentifizierungsmechanismen (wie z. B. NTLM und Kerberos), die ein höheres Maß an Sicherheit bieten und das Kennwort nicht über das Netzwerk in Klartext senden.

Wenn die virtuellen Front-End-HTTP-Server Anfragen authentifizieren, werden vom Benutzer Authentifizierungsinformationen angefordert. Der Benutzer sendet Authentifizierungsinformationen an den Front-End-Server, der den Benutzer authentifiziert und dann die Informationen an den Back-End-Server weiterleitet. Der Back-End-Server authentifiziert anschließend den Benutzer, muss jedoch nicht erneut Authentifizierungsinformationen vom Benutzer abrufen.

- Exchange 2000-Front-End-Server verwenden Standardauthentifizierung für den HTTP-Zugriff auf den Back-End-Server.
- Exchange 2003-Front-End-Server verwenden integrierte Authentifizierung für den HTTP-Zugriff auf den Back-End-Server.

Nur Internet Explorer bietet direkte Unterstützung für die integrierte Windows-Authentifizierung für einen Back-End-Server.

Erstellen und Konfigurieren von virtuellen HTTP-Servern auf Back-End-Servern

Unter Konfigurieren von Exchange-Front-End-Servern werden zwei Methoden zur Konfiguration der Front-End- und Back-End-Topologie beim Hosten von mehreren Domänen erläutert:

- Methode eins beinhaltet das Einrichten eines virtuellen Servers für alle gehosteten Domänen.
- Methode zwei beinhaltet das Einrichten eines virtuellen Verzeichnisses für alle gehosteten Domänen.

Die Back-End-Konfiguration unterscheidet sich je nach Auswahl der Methode in einigen wenigen Punkten. Wenn Sie aus anderen Gründen zusätzliche virtuelle Server auf den Front-End-Servern erstellen, zum Beispiel zum Hosten von Webanwendungen, müssen Sie ähnlich konfigurierte virtuelle Server allen Back-End-Servern hinzufügen, auf denen die Webanwendungen ausgeführt werden sollen.

Methode eins: Konfigurieren von zusätzlichen virtuellen Servern

Wenn Sie einen zusätzlichen virtuellen Server für jede weitere Domäne erstellen möchten (mit einem virtuellen Exchange-Verzeichnis unterhalb jeder weiteren Domäne), müssen Sie einen übereinstimmenden virtuellen Server auf dem Back-End-Server erstellen. Die Schritte bei der Konfiguration des Front-End-Servers weichen leicht von denjenigen des Back-End-Servers ab..

Ausführliche Anweisungen zum Konfigurieren zusätzlicher virtueller Server auf einem Back-End-Server finden Sie unter Konfigurieren von zusätzlichen virtuellen Servern auf einem Back-End-Server.

Methode zwei: Erstellen zusätzlicher virtueller Verzeichnisse

Wenn Sie zusätzliche virtuelle Verzeichnisse (unter der Standarddomäne) für jede weitere Domäne erstellen möchten, konfigurieren Sie die virtuelle Verzeichnisstruktur so, dass sie mit der Verzeichnisstruktur auf den Front-End-Servern übereinstimmt. Stellen Sie wie bei den Front-End-Servern sicher, dass die jeweilige SMTP-Domäne für virtuelle Verzeichnisse, die mit den Postfachspeichern verknüpft sind, angeben.

Der Verzeichnisname darf die folgenden Zeichen nicht enthalten, da sie von IIS blockiert werden: Punkt (.), Doppelpunkt (..), Punkt und Schrägstrich (./), Umgekehrter Schrägstrich (\), Prozentzeichen (%), Kaufmännisches Und (&).

Konfigurieren von zusätzlichen virtuellen Servern auf einem Back-End-Server

Wenn Sie zusätzliche virtuelle Server auf Ihren Exchange-Front-End-Server erstellen, müssen Sie den Back-End-Servern ähnlich konfigurierte virtuelle Server hinzufügen. In diesem Verfahren wird die Konfiguration zusätzlicher virtueller Server auf einem Back-End-Server erläutert.

Bevor Sie beginnen

Bevor Sie die Verfahren in diesem Thema ausführen, müssen Sie einen zusätzlichen virtuellen Server auf Ihrem Front-End-Server erstellen. Weitere Informationen zum Erstellen von zusätzlichen virtuellen Servern auf Ihrem Front-End-Server finden Sie unter Konfigurieren von Exchange-Front-End-Servern.

Verfahren

So konfigurieren Sie einen zusätzlichen Server auf Ihrem Back-End-Server

1. Starten Sie den Exchange-System-Manager: Klicken Sie auf **Start**, zeigen Sie auf **Programme** und anschließend auf **Microsoft Exchange**, und klicken Sie dann auf **System-Manager**.
2. Wenn administrative Gruppen im Exchange-System-Manager angezeigt werden, erweitern Sie **Administrative Gruppen**, erweitern Sie **Server**, und erweitern Sie anschließend den Server, für den Sie die Verwendung einer E-Mail-Adresse als Anmeldename des Benutzers konfigurieren möchten.
3. Erweitern Sie **Protokolle**, klicken Sie mit der rechten Maustaste auf **HTTP**, klicken Sie auf **Neu**, und wählen Sie dann **Virtueller HTTP-Server** aus.
4. Geben Sie im Dialogfeld **Eigenschaften** einen Namen für den virtuellen Server ein. Geben Sie dem virtuellen Server einen konsistenten Namen, wie zum Beispiel "adatum.com (back-end)".
5. Klicken Sie unter **Exchange-Pfad** auf **Ändern**, wählen Sie die gewünschte Domäne aus der Liste aus (in diesem Fall adatum.com), und klicken Sie auf **OK**.
6. Klicken Sie auf **Erweitert**, und fügen Sie den gewünschten Hostnamen hinzu (in diesem Fall mail.adatum.com) Die Adresse, mit der der Clientbrowser auf den Front-End-Server zugreift, wird vom Front-End-Server an den Back-End-Server weitergeleitet, so dass der Back-End-Server alle vom Client verwendeten Namen für den Zugriff auf den Front-End-Server kennt (zum Beispiel http://mail, http://mail.adatum.com usw.).

Hinweis:

Auf dem Back-End-Server muss TCP-Anschluss 80 geöffnet sein. Dies ist der einzige Anschluss, der zur Kommunikation zwischen Front- und Back-End-Server verwendet wird, unabhängig davon, welcher Anschluss vom Client für die Kommunikation mit dem Front-End-Server verwendet wird). Sie können die Standardeinstellung für den SSL-Anschluss beibehalten.

Konfigurieren von Firewalls

In diesem Abschnitt wird die Konfiguration von Firewalls zur Verwendung mit einer Exchange-Front-End- und Back-End-Topologie erläutert. Die folgenden Themen bieten zusätzliche Konfigurationsinformationen zu Front-End-Servern in diesen Umgebungen.

- Konfigurieren einer Internetfirewall
- Konfigurieren einer Intranetfirewall

Konfigurieren einer Internetfirewall

In Internet-Szenarien wird eine Firewall normalerweise zwischen dem Unternehmensnetzwerk und dem Internet positioniert. Die Firewall steuert die Verbindungen, die zwischen den Computern im Internet und den Computern im Unternehmensnetzwerk erlaubt sind. Beim Konfigurieren dieser Firewall muss die Richtung des Datenverkehrs beachtet werden. Detaillierte Informationen zur Anschlussrichtung finden Sie unter "Anschlussfilterung" in Verwenden von Firewalls in einer Front-End- und Back-End-Topologie.

Konfigurieren Sie die Firewall, um Anfragen an bestimmte IP-Adressen sowie über bestimmte TCP/IP-Anschlüsse zu ermöglichen. In der folgenden Tabelle finden Sie eine Auflistung der für bestimmte Dienste erforderlichen Anschlüsse. Diese Anschlüsse beziehen sich auf eingehenden Datenverkehr (vom Internet an den Front-End-Server).

Anschlüsse, die auf der Internetfirewall geöffnet sein müssen

Zielanschlussnummer/-transport	Protokoll
443/TCP - eingehend	HTTPS (SSL-gesichertes HTTP)
993/TCP - eingehend	SSL-gesichertes IMAP
995/TCP - eingehend	SSL-gesichertes POP

Zielanschlussnummer/-transport	Protokoll
25/TCP - eingehend	SMTP

Hinweis:

"Eingehend" in dieser Tabelle bedeutet, dass Sie die Firewall so konfiguriert sollten, dass Computer von außen (in diesem Fall im Internet) Verbindungen zum Front-End-Server herstellen können. Der Front-End-Server stellt nie Verbindungen zu Computern im Internet her. Er antwortet lediglich auf Verbindungsanfragen von Computern im Internet.

Konfigurieren von ISA Server

Bei Verwendung von ISA Server sind folgende Konfigurationseinstellungen erforderlich. (Dies sind allgemeine Richtlinie. Detaillierte Informationen zum Konfigurieren von ISA Server finden Sie in der Produktdokumentation.)

1. Konfigurieren Sie einen Listener für SSL.
2. Erstellen Sie ein Zielset mit der externen IP-Adresse des ISA-Servers. Dieses Zielset wird in der Web-Veröffentlichungsregel festgelegt.
3. Erstellen Sie eine Web-Veröffentlichungsregel, die die Anfragen an den internen Front-End-Server umleitet.
4. Erstellen Sie Protokollregeln, um die Anschlüsse in ISA Server für ausgehenden Datenverkehr zu öffnen.
5. Konfigurieren Sie den ISA-Server für Outlook Web Access. Informationen zum Konfigurieren eines ISA-Servers für Outlook Web Access finden Sie im Microsoft Knowledge Base-Artikel 307347, "Sichere OWA-Veröffentlichung hinter ISA Server kann benutzerdefinierten HTTP-Header erfordern."

Konfigurieren einer Intranetfirewall

In diesem Thema wird die Verwendung eines Umgebungsnetzwerk mit einer externen und internen Firewall erläutert. Die folgenden Abschnitte beinhalten Erläuterungen zur Konfiguration des Umgebungsnetzwerks, der Intranetfirewall und des ISA-Servers zur ordnungsgemäßen Ausführung von Exchange.

Neu in SP2 Mit Microsoft® Exchange Server 2003 Service Pack 2 (SP2) hat Microsoft eine Direct Push-Technologie eingeführt, mit der Exchange ActiveSync® E-Mail-Nachrichten direkt an das mobile Geräte weiterleitet kann, sobald diese den Server erreichen. Mit der Direct Push-Technologie sendet der Back-End-Server immer, wenn er eine an das mobile

Gerät zu übertragende E-Mail-Nachricht empfängt, eine UDP-Benachrichtigung an den Front-End-Server. Für diese Übertragung muss der UDP-Anschluss 2883 auf der Firewall geöffnet sein, um Datenverkehr in eine Richtung vom Back-End-Server zum Front-End-Server zuzulassen.

Weitere Informationen zur Bereitstellung der Direct Push-Technologie und den Auswirkungen auf die Firewallkonfiguration finden Sie im Exchange Server-Blogartikel

- Direct Push is just a heartbeat away.

Hinweis:

Die Inhalte der einzelnen Blogartikel und ihren URL können ohne vorherige Ankündigung geändert werden.

Erweiterter Firewallserver in einem Umgebungsnetzwerk

Wenn es sich bei Ihrem erweiterten Firewallserver (zum Beispiel ISA) nicht auch um Ihre Intranetfirewall handelt (zwischen dem erweiterten Firewallserver und dem Front-End-Server ist eine zusätzliche Firewall vorhanden), müssen Sie die erforderlichen Protokollanschlüsse auf Ihrer Intranetfirewall öffnen, um dem erweiterten Firewallserver die Weiterleitung von Anfragen zu ermöglichen.

Zur Weiterleitung von Anfragen über den erweiterten Firewallserver erforderlichen Protokollanschlüsse

Zielanschlussnummer/-transport	Protokoll
443/TCP - eingehend oder 80/TCP - eingehend	HTTPS (SSL-gesichertes HTTP) oder HTTP, je nachdem, ob die erweiterte Firewall (wie zum Beispiel ISA) die SSL-Entschlüsselung verschiebt
993/TCP - eingehend	SSL-gesichertes IMAP
995/TCP - eingehend	SSL-gesichertes POP
25/TCP - eingehend	SMTP

Zusätzliche Anschlüsse sind möglicherweise erforderlich, wenn die erweiterte Firewall bestimmte Tasks wie die Authentifizierung von Benutzern ausführt. Weitere Informationen finden Sie in der Dokumentation zu Ihrer erweiterten Firewall.

Hinweis:

Von anderen Firewallanbietern werden möglicherweise weitere Konfigurationseinstellungen zur IP-Fragmentierung für die jeweiligen Produkte empfohlen.

Front-End-Server in einem Umgebungsnetzwerk

In einem Umgebungsnetzwerk muss der Front-End-Server in der Lage sein, Verbindungen zu Back-End-Servern und Active Directory® -Verzeichnisdienstservern herzustellen. Konfigurieren Sie daher Ihre interne Firewall mit einer Regel, die eingehenden Datenverkehr über Anschluss 80 vom Umgebungsnetzwerk zum Unternehmensnetzwerk erlaubt. Diese Regel verweigert jedoch ausgehenden Datenverkehr über Anschluss 80 vom Unternehmensnetzwerk zum Front-End-Server. Die folgende Diskussion über Anschlüsse bezieht sich auf Eingangsanschlüsse, über die der Datenverkehr vom Server in einem Umgebungsnetzwerk zu den Back-End-Servern erfolgt.

Hinweis:

Die bevorzugte Bereitstellungsmethode für den Front-End-Server ist die Positionierung im Intranet mit den Back-End-Servern und die Verwendung einer erweiterten Firewall als Umgebungsnetzwerk. Lesen Sie diesen Abschnitt, wenn zur Positionierung des Exchange-Front-End-Servers im Umgebungsnetzwerk bestimmte Anforderungen bestehen.

Standardprotokolle

Alle unterstützten Protokollanschlüsse müssen in der inneren Firewall immer geöffnet sein. Die SSL-Anschlüsse müssen nicht geöffnet sein, da SSL zur Kommunikation zwischen dem Front-End-Server und den Back-End-Servern nicht verwendet wird. In der folgenden Tabelle finden Sie eine Auflistung der für die Intranetfirewall erforderlichen Anschlüsse Diese Anschlüsse sind spezifisch für eingehenden Datenverkehr (vom Front-End-Server zu den Back-End-Servern).

Für die Intranetfirewall erforderliche Protokollanschlüsse

Anschlussnummer/-transport	Protokoll
80/TCP - eingehend	HTTP
143/TCP - eingehend	IMAP
110/TCP - eingehend	POP
25/TCP - eingehend 691/TCP	SMTP Routing des Verbindungsstatusalgorithmus

Hinweis:

In dieser Tabelle bedeutet "eingehend", dass die Firewall zum Zulassen von Computern (zum Beispiel erweiterte Firewallserver) im Umgebungsnetzwerk konfiguriert werden sollte, um Verbindungen vom Front-End-Server im Unternehmensnetzwerk herzustellen. Der Front-End-Server muss nie Verbindungen zu Computern in einem Umgebungsnetzwerk herstellen. Der Front-End-Server reagiert lediglich auf Verbindungen, die von Computern im Umgebungsnetzwerk initiiert wurden.

Active Directory-Kommunikation

Zur Kommunikation mit Active Directory müssen die LDAP-Anschlüsse auf dem Exchange-Front-End-Server geöffnet sein. TCP und UDP sind erforderlich. Windows auf dem Front-End-Server sendet eine 389/UDP-LDAP-Anfrage an einen Domänencontroller, um dessen Verfügbarkeit zu überprüfen. Anschließend verwendet der LDAP-Datenverkehr TCP. Die Windows Kerberos-Authentifizierung wird ebenfalls verwendet. Der Kerberos-Anschluss muss daher ebenfalls geöffnet sein. TCP und UDP sind ebenfalls für Kerberos erforderlich. Windows verwendet standardmäßig UDP/88. Wenn die Datenmenge die maximale Paketgröße für UDP übersteigt, kommt TCP zum Einsatz. In der folgenden Tabelle werden die zur Kommunikation mit Active Directory und Kerberos benötigen Anschlüsse aufgelistet.

Zur Kommunikation mit Active Directory und Kerberos benötigten Anschlüsse

Anschlussnummer/-transport	Protokoll
389/TCP	LDAP zum Verzeichnisdienst
389/UDP	
3268/TCP	LDAP zum globalen Katalogserver
88/TCP	Kerberos-Authentifizierung
88/UDP	

Auf der Firewall können zwei optionale Anschlusssets geöffnet werden. Die Auswahl richtet sich nach den jeweiligen Richtlinien des Unternehmens. Jede Entscheidung bringt jedoch auch Nachteile in den Bereichen Sicherheit, einfache Verwaltung und Funktionalität.

DNS (Domain Name Service)

Der Front-End-Server muss auf einen DNS-Server zugreifen, um Servernamen ordnungsgemäß zu ermitteln (z. B. zum Konvertieren von Servernamen in IP-Adressen). In der folgenden Tabelle werden die für diesen Zugriff erforderlichen Anschlüsse aufgelistet.

Wenn Sie diese Anschlüsse nicht öffnen möchten, müssen Sie einen DNS-Server auf dem Front-End-Server installieren und den richtigen Namen für IP-Zuordnungen für alle Server eingeben, zu denen möglicherweise eine Verbindung hergestellt wird. Weiterhin müssen alle Active Directory SRV-Datensätze konfigurieren, da der Front-End-Server in der Lage sein muss, Domänencontoller zu ermitteln. Stellen Sie bei der Installation eines DNS-Servers sicher, dass diese Zuordnungen bei Änderungen an der Organisation aktualisiert werden.

Für den Zugriff auf den DNS-Server erforderliche Anschlüsse

Anschlussnummer/-transport	Protokoll
53/TCP	DNS-Suche
53/UDP	

Hinweis:

Die meisten Dienst setzen UDP für die DNS-Suche ein. TCP wird nur verwendet, wenn der Umfang der Anfrage die maximale Paketgröße übersteigt. Der Exchange SMTP-Dienst verwendet TCP jedoch standardmäßig für die DNS-Suche. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 263237 mit Informationen zur Verwendung von TCP-DNS-Anfragen in Windows 2000- und Exchange 2000-SMTP.

IPSec

In der folgenden Tabelle werden die für den IPSec-Datenverkehr über die Intranetfirewall benötigten Anforderungen aufgelistet: Sie müssen nur den Anschluss für das Protokoll aktivieren, das Sie konfigurieren. Wenn Sie zum Beispiel ESP verwenden, müssen Sie nur das IP-Protokoll 50 über die Firwall zulassen.

Für IPSec benötigte Anschlüsse

Anschlussnummer/-transport	Protokoll
IP-Protokoll 51	AH (Authentication Header)
IP-Protokoll 50	ESP (Encapsulating Security Payload)
500/UDP	IKE (Internet Key Exchange)
88/TCP	Kerberos
88/UDP	

RPCs (Remote Procedure Calls)

DSAccess verwendet RPCs nicht mehr zum Ermitteln von Active Directory-Diensten. Da Ihr Front-End-Server jedoch zur Authentifizierung von Anfragen konfiguriert ist, muss IIS nach wie vor RPC-Zugriff auf Active Directory haben, um Anfragen zu authentifizieren. Öffnen Sie daher die RPC-Anschlüsse, die in der Tabelle "Zur Authentifizierung benötigte RPC-Anschlüsse" weiter unten aufgelistet sind.

Beenden von RPC-Datenverkehr

Wenn Sie über ein eingeschränktes Umgebungsnetzwerk verfügen, in dem der Front-End-Server keine Benutzer authentifizieren kann, können Sie möglicherweise die in der Tabelle "Zur Authentifizierung benötigte RPC-Anschlüsse" weiter unten aufgelisteten RPC-Anschlüsse nicht öffnen. Ohne diese RPC-Anschlüsse kann der Front-End-Server jedoch keine Authentifizierung durchführen. Sie können den Front-End-Server für den anonymen Zugriff konfigurieren, Sie sollten sich jedoch über die dabei entstehenden Risiken bewusst sein. Weitere Informationen finden Sie unter Authentifizierungsmechanismen für HTTP.

Um das Beenden des gesamten RPC-Datenverkehrs zu vermeiden, wird empfohlen, den RPC-Datenverkehr durch Öffnen eines Anschlusses (wie im folgenden Abschnitt beschrieben) zu beschränken.

Beschränken des RPC-Datenverkehrs

Wenn Sie die für RPCs benötigten Features, wie zum Beispiel Authentifizierung oder implizite Anmeldung, konfigurieren möchten, die breite Palette von Anschlüssen über 1024 jedoch nicht öffnen möchten, können Sie Ihre Domänencontroller und globalen Katalogserver zur Verwendung eines einzelnen Anschlusses für den gesamten RPC-Datenverkehr konfigurieren. Weitere Informationen zur Beschränkung von RPC-Datenverkehr finden Sie im Microsoft Knowledge Base-Artikel 224196, "Einschränken von Active Directory-Replikationsverkehr an einem bestimmten Port."

Zur Clientauthentifizierung muss der Registrierungsschlüssel (wie im oberen Knowledge Base-Artikel und im Folgenden erläutert) auf allen Servern festgelegt werden, die der Front-End-Server möglicherweise kontaktiert (zum Beispiel ein globaler Katalogserver). Legen Sie den folgenden Registrierungsschlüssel für einen bestimmten Anschluss fest, zum Beispiel 1600:

HKEY_LOCAL_MACHINE\CurrentControlSet\Services\NTDS\Parameters

Registrierungswert: TCP/IP-Port Werttyp: REG_DWORD-Wertdaten: (verfügbarer Anschluss)

Öffnen Sie auf der Firewall zwischen dem Umgebungsnetzwerk und Ihrem Intranet lediglich die beiden Anschlüsse für die RPC-Kommunikation - Der RPC-Portmapper (135) und der von Ihnen angegebene Anschluss (Anschluss 1600, wie in der folgenden Tabelle

angegeben). Der Front-End-Server versucht zunächst, die Back-End-Server mit RPCs über Anschluss 135 zu kontaktieren, und der Back-End-Server antwortet mit dem aktuell verwendeten RPC-Anschluss.

Hinweis:

Exchange-System-Administrator verwendet RPCs zur Verwaltung von Exchange-Servern. Es wird empfohlen, dass Sie Exchange-System-Administrator auf einem Front-End-Server nicht zur Verwaltung von Back-End-Servern einsetzen, da hierfür die Konfiguration von RPC-Zugriff vom Front-End-Server zu jedem einzelnen Back-End-Server erforderlich ist. Verwenden Sie Exchange-System-Administrator über einen Exchange-Clientcomputer oder einen Back-End-Server, um Back-End-Server zu verwalten. Sie können jedoch Exchange-System-Administrator nach wie vor auf dem Front-End-Server zur Verwaltung des Front-End-Servers selbst verwenden.

Zur Authentifizierung benötigte RPC-Anschlüsse

Anschlussnummer/-transport	Protokoll
135/TCP	Endpunktzuordnung für RPC-Anschlüsse
1024+/TCP Oder 1600/TCP	Zufällige Dienstanschlüsse (Beispiel) Bestimmter RPC-Dienstanschluss, falls beschränkt

Front-End- und Back-End-Topologie - Prüfliste

In der folgenden Prüfliste werden die zur Konfiguration von Front-End-Servern, Back-End-Servern und Firewalls erforderlichen Schritte zusammengefasst.

Hinweis:

Die folgenden Verfahren beinhalten Informationen zum Editieren der Registrierung. Die fehlerhafte Verwendung des Registrierungs-Editors kann zu ernsthaften Problemen führen, die möglicherweise eine Neuinstallation des Betriebssystems erforderlich machen. Microsoft übernimmt keine Garantie dafür, dass durch unsachgemäßes Verwenden des Registrierungs-Editors verursachte Probleme behoben werden können. Sie verwenden den Registrierungs-Editor auf eigene Verantwortung. Informationen zum Bearbeiten der Registrierung finden Sie unter "Ändern von Schlüsseln und Werten" in der Hilfe zum Registrierungs-Editor (Regedit.exe) oder unter "Hinzufügen und Löschen von Daten in der Registrierung" und "Bearbeiten der Registrierungsdaten" in der Hilfe zu Regedt32.exe Beachten

Sie, dass die Registrierung vor der Bearbeitung gesichert werden sollte. Sie sollten ebenfalls Ihre Notfalldiskette aktualisieren.

Hinweis:

In den folgenden Tabellen werden Aufgaben für die Front-End- und Back-End-Topologie in Form einer Prüfliste dargestellt.

Konfigurieren der Front-End-Server

Aufgabe
Schritt 1. Installieren Sie Exchange Server: Installieren Sie Exchange Server auf dem Front-End-Server.
Schritt 2. Konfigurieren Sie virtuelle HTTP-Server oder -Verzeichnisse auf dem Front-End-Server für den Zugriff auf Postfachspeicher und Informationspeicher für Öffentilche Ordner je nach Bedarf: Geben Sie für zusätzliche virtuelle Server die SMTP-Domäne, IP-Adresse und Hostheader oder Anschlüsse an. Behalten Sie die Aktivierung des Kontrollkästchens **Standardauthentifizierung** bei. Geben Sie für zusätzliche virtuelle Verzeichnisse für öffentliche Informationsspeicher das jeweilige Stammverzeichnis für öffentliche Informationsspeicher an. Geben Sie für zusätzliche virtuelle Verzeichnisse für Postfachspeicher die SMTP-Domäne an.
Schritt 3. Deaktivieren Sie nicht benötigte Dienste: Beenden Sie alle Dienste, die für die verwendeten Protokolle nicht benötigt werden.
Schritt 4. Deaktivieren oder löschen Sie nach Bedarf alle Informationsspeicher: Wenn Sie SMTP nicht ausführen, deaktivieren oder löschen Sie alle Postfachspeicher. Wenn Sie SMTP ausführen, behalten Sie einen Postfachspeicher bei, stellen Sie jedoch sicher, dass der Postfachspeicher keine Postfächer enthält. Wenn Sie viele externe E-Mail-Nachrichten erhalten, können Sie einen öffentlichen Informationsspeicher bereitstellen, da dies die Nachrichtenübermittlung an Öffentliche Ordner verbessert.
Schritt 5. Richten Sie bei Bedarf den Lastenausgleich für Front-End-Server ein: Installieren Sie den Lastenausgleich auf allen Front-End-Servern. (Empfohlen) Aktivieren Sie Clientaffinität.

Aufgabe
Schritt 6. Konfigurieren Sie SSL (empfohlen): Option 1: Konfigurieren Sie SSL auf dem Front-End-Server. Option 2: Richten Sie einen Server zwischen dem Client und dem Front-End-Server ein, um SSL-Entschlüsselung zu verschieben.
Schritt 7. Bei Verwendung eines Umgebungsnetzwerks: **Hinweis:** Bei diesem Verfahren empfiehlt es sich, einen erweiterten Firewallserver (wie zum Beispiel ISA Server) anstelle des Front-End-Servers im Umgebungsnetzwerk einzusetzen. Weitere Informationen finden Sie unter Erweiterte Firewall in einem Umgebungsnetzwerk. Erstellen Sie den Registrierungsschlüssel **DisableNetlogonCheck**, und setzen Sie den REG_DWORD-Wert auf **1**. Erstellen Sie den Registrierungsschlüssel **LdapKeepAliveSecs**, und setzen Sie den REG_DWORD-Wert auf **0**. Wenn Sie den Front-End-Server auf die Kontaktierung bestimmter Domänencontroller und globaler Katalogserver beschränken möchten, geben Sie diese im Exchange-System-Manager auf dem Front-End-Server ein.
Schritt 8. Bei Verwendung eines Umgebungsnetzwerks und Verweigerung von RPCs über die Intranetfirewall: **Hinweis:** Wenn Sie die Authentifizierung auf dem Front-End-Server deaktivieren möchten, können anonyme Anfragen Ihre Back-End-Server erreichen. Deaktivieren Sie die Authentifizierung auf dem Front-End-Server.
Schritt 9. Erstellen Sie bei Bedarf eine IPSec-Richtlinie auf den Front-End-Servern.

Konfigurieren der Back-End-Server

Aufgaben
1. Erstellen und konfigurieren Sie virtuelle HTTP-Server oder -Verzeichnisse, die mit dem Front-End übereinstimmen: 2. Legen Sie für zusätzliche virtuelle Server den Hostheader und die IP-Adressen entsprechend fest. Der TCP-Anschluss 80 muss beibehalten werden. Stellen Sie sicher, dass die Kontrollkästchen **Standardauthentifizierung** und **Integrierte Windows-Authentifizierung** aktiviert sind. 3. Geben Sie für zusätzliche virtuelle Verzeichnisse für Informationsspeicher für Öffentliche Ordner das entsprechende Stammverzeichnis für den Informationsspeicher für Öffentliche Ordner an, das dem auf dem Front-End-Server konfigurierten Stammverzeichnis entspricht. 4. Geben Sie für zusätzliche virtuelle Verzeichnisse für Postfachspeicher die SMTP-Domäne an.

Konfigurieren von Firewalls

Aufgabe
Schritt 1. Konfigurieren Sie die Internetfirewall (zwischen dem Internet und den Front-End-Servern): Öffnen Sie die TCP-Anschlüsse auf der Internetfirewall für die E-Mail-Protokolle: 443 für HTTPS 993 für SSL-fähiges IMAP 995 für SSL-fähiges POP 25 für SMTP (einschließlich TLS)

Aufgabe
Schritt 2. (Fortsetzung) Führen Sie bei Verwendung von ISA Server die folgende Konfiguration aus: Konfigurieren Sie einen Listener für SSL. Erstellen Sie ein Zielset mit der externen IP-Adresse des ISA-Servers. Dieses Zielset wird in der Web-Veröffentlichungsregel festgelegt. Erstellen Sie eine Web-Veröffentlichungsregel, die die Anfragen an den internen Front-End-Server umleitet. Erstellen Sie Protokollregeln, um die Anschlüsse in ISA Server für ausgehenden Datenverkehr zu öffnen. Konfigurieren Sie den ISA-Server für Outlook Web Access (weitere Informationen zum Konfigurieren eines ISA-Servers für Outlook Web Access finden Sie im Microsoft Knowledge Base-Artikel 307347, "Sichere OWA-Veröffentlichung hinter ISA Server kann benutzerdefinierten HTTP-Header erfordern."

Aufgabe
Schritt 3. Konfigurieren Sie die Intranetfirewall bei Verwendung eines Front-End-Servers in einem Umgebungsnetzwerk: Öffnen Sie die TCP-Anschlüsse auf der Intranetfirewall für die verwendeten Protokolle: • 80 für HTTP • 143 für IMAP • 110 für POP • 25 für SMTP • 691 für das LSA (Link State Algorithm, Verbindungsalgorithmus)-Routingprotokoll Öffnen Sie Anschlüsse für die Active Directory-Kommunikation • TCP-Anschluss 389 für LDAP zum Verzeichnisdienst • UDP-Anschluss 389 für LDAP zum Verzeichnisdienst • TCP-Anschluss 3268 für LDAP zum globalen Katalogserver • TCP-Anschluss 88 für Kerberos-Authentifizierung • UDP-Anschluss 88 für Kerberos-Authentifizierung Öffnen Sie die für den Zugriff auf den DNS-Server erforderlichen Anschlüsse: • TCP-Anschluss 53 • UDP-Anschluss 53 Öffnen Sie die entsprechenden Anschlüsse für die RPC-Kommunikation: • TCP-Anschluss 135 - RPC-Endpunktzuordnung • TCP-Anschlüsse 1024+ - zufällige RPC-Dienstanschlüsse (Optional) Bearbeiten Sie zum Beschränken der RPCs über die Intranetfirewall die Registrierung auf den Servern im Intranet, um RPC-Datenverkehr für einen bestimmten, nicht zufälligen Anschluss festzulegen. Öffnen Sie anschließend die gewünschten Anschlüsse auf der internen Firewall: • TCP-Anschluss 135 - RPC-Endpunktzuordnung • TCP-Anschluss 1600 (Beispiel) – RPC-Dienstanschluss Wenn Sie IPSec zwischen dem Front-End und dem Back-End verwenden, öffnen Sie die entsprechenden Anschlüsse. Wenn die von Ihnen konfigurierte Richtlinie nur AH verwendet, müssen Sie ESP nicht zulassen und umgekehrt. • UDP-Anschluss 500 – IKE • IP-Protokoll 51 – AH • IP-Protokoll 50 – ESP • UDP-Anschluss 88 und TCP-Anschluss 88 – Kerberos

Problembehandlung in einer Front-End- und Back-End-Topologie

Probleme bei Front-End- und Back-End-Architekturen werden häufig dadurch verursacht, dass der Netzwerkverkehr aufgrund von falschen Konfigurationen auf dem Server oder den Netzwerkroutern nicht vom Front-End-Server zu den richtigen Back-End-Servern weitergeleitet wird. Detaillierte Informationen zu den jeweiligen Probleme finden Sie in den Ereignisprotokolleinträgen. Im folgenden Abschnitt finden Sie mögliche Problembehandlungsstrategien für Ihre Front-End- und Back-End-Topologie.

Problembehandlungstools

Beim Behandeln von Problemen in einer Front-End- und Back-End-Topologie können die folgenden Tools hilfreich sein:

- **Netzwerkmonitor** Verwenden Sie den Netzwerkmonitor zur Überwachung des Datenverkehrs sowie zur genauen Beobachtung der Vorgänge zwischen dem Front-End-Server und anderen Servern. Richten Sie einen Client ein, um eine Verbindung zum Front-End-Server herzustellen, und überwachen den Datenverkehr zwischen den Front-End-Servern und den Intranetservern. Der Netzwerkmonitor kann ebenfalls zur Überwachung der Client- und Front-End-Serververbindung eingesetzt werden, wenn SSL nicht verwendet wird.
- **Ereignisanzeige** Überprüfen Sie die Ereignisprotokolle auf den Front-End- und Back-End-Servern sowie alle anderen beteiligten Server (DNS-Server, globale Katalogserver und andere). In den jeweiligen Einträgen erhalten Sie möglicherweise Informationen zur Ursache des Problems.
- **RPC-Ping** Verwenden Sie zum Testen der RPC-Konnektivität zwischen dem Front-End-Server und einem globalen Katalogserver bzw. Back-End-Server das Tool **Rpings.exe**. Dieses Tool ist im Supportverzeichnis der Exchange-CD enthalten.
- **Telnet** Verwenden Sie **telnet.exe**, um eine direkte Verbindung zum Back-End-Server des Benutzers über den Anschluss, den das E-Mail-Protokoll verwendet, herzustellen. Wenn Outlook Web Access beim Herstellen einer Verbindung zum Front-End-Server nicht reagiert, verwenden Sie Telnet auf dem Front-End-Server, um über Anschluss 80 auf den Back-End-Server zu gelangen.

Allgemeine Fehlerbehandlungsschritte

- Stellen Sie sicher, dass die richtigen Dienste auf den Front-End- und Back-End-Servern gestartet sind. Darin enthalten sind die jeweiligen Exchange-Dienste sowie der WWW-Publishingdienst und der SMTP-Dienst (falls erforderlich).
- Stellen Sie bei einem Umgebungsnetzwerk sicher, dass die richtigen Anschlüsse auf der internen Firewall wie unter Konfigurieren von Firewalls beschrieben geöffnet sind.
- Stellen Sie weiterhin sicher, dass der Front-End-Server eine Verbindung zu den globalen Katalogservern sowie zum DNS-Server herstellen kann. Dies ist besonders von Bedeutung, wenn sich der Front-End-Server in einem Umgebungsnetzwerk befindet. Verwenden Sie Telnet vom Front-End-Server zu den jeweiligen Anschlüssen auf den Servern im Intranet: 389, 3268, 53 und weitere Anschlüsse.

  Hinweis:

  Windows Telnet verwendet TCP/IP und kann für Verbindungen zu UDP-Anschlüssen nicht verwendet werden.
- Wenn Sie mit dem Hostnamen und einem beliebigen Protokoll keine Verbindung vom Back-End-Server zum Front-End-Server herstellen können, verwenden Sie die IP-Adresse. Überprüfen Sie bei erfolgreichem Verbindungsaufbau, ob Sie eine Verbindung zum DNS-Server herstellen können, der vom Front-End-Server verwendet wird. Stellen Sie ebenfalls sicher, dass die IP-Zuordnung in DNS ordnungsgemäß durchgeführt wurde.
- Wenn der Front-End-Server mit der Liste der Domänencontroller und globalen Katalogservern in der Registrierung konfiguriert wurde, überprüfen Sie, ob der Front-End-Server alle Server genau so erreicht, wie im Registrierungseintrag angegeben.
- Stellen Sie sicher, dass die Kombination aus IP-Adresse und Hostheader für jeden einzelnen Server eindeutig ist.
- Wenn Sie eine Lastenausgleichslösung für die Front-End-Server einsetzen, stellen Sie sicher, dass die Clientcomputer auf die freigegebene IP-Adresse zugreifen können.
- Verwaltung: Stellen Sie bei Verwendung von Exchange-System-Manager sicher, dass der Systemaufsichtsdienst ausgeführt wird. Erinnern Sie sich ebenfalls daran, dass Sie den Internetdienste-Manager nach dem Löschen der Speicher auf dem Front-End-Server nicht verwenden können.
- Wenn sich Benutzer über den in kurzen Abständen wechselnden Status von gelesenen und ungelesenen Nachrichten beschweren, stellen Sie sich die folgenden Fragen:
  - Wurde auf dem Back-End-Server ein Öffentlicher Ordner hinzugefügt oder entfernt?
  - Ist die Authentifizierung auf dem Front-End-Server aktiviert?
  - Reagieren bestimmte Back-End-Server nicht mehr, die den Öffentlichen Ordner hosten?

Anmeldungsfehlschläge

Wenn Ihre Benutzer Probleme bei der Anmeldung an POP, IMAP oder Outlook Access haben, hat dies häufig folgende Ursachen:

- Gibt der Benutzer den Benutzernamen im richtigen Format ein? (*domäne\benutzername, benutzername@domäne.com, benutzername*)
- Wenn UPN oder eine Standarddomäne konfiguriert ist und der Benutzer den Benutzernamen im richtigen Format eingibt, überprüfen Sie, ob die Domäneneinstellung auf allen virtuellen Servern und Verzeichnissen im Exchange-System-Manager richtig ist. Überprüfen Sie dieselbe Einstellung im Internetdienste-Manager. Wenn die Domäneneinstellung im Exchange-System-Manager richtig ist, im Internetdienste-Manager jedoch nicht, liegt dies wahrscheinlich an der fehlerhaften Replikation der Einstellungen vom Exchange-System-Manager zum Internetdienste-Manager. Starten Sie den MSExchangeSA-Dienst neu, um das Problem zu beheben.
- Stellen Sie sicher, dass die Hostheader für den virtuellen HTTP-Server den Einstellungen entspricht, die der Browser für den Verbindungsaufbau zum Server verwendet. Stellen Sie weiterhin sicher, dass die Hostheader und die Eingabe auf den virtuellen Back-End- und Front-End-Servern bzw. in den Verzeichnissen fehlerfrei sind.
- Wenn Sie über mehrere virtuelle Server für mehrere Domänen verfügen, stellen Sie sicher, dass die SMTP-Domäne ordnungsgemäß konfiguriert ist.
- Stellen Sie sicher, dass der sich anmeldende Benutzer eine E-Mail-Adresse für die Domäne hat, die für den virtuellen Server, auf den der Benutzer zugreift, konfiguriert ist.

Fehlerbehandlung in Outlook Web Access

Ausführliche Informationen zur Problembehandlung in Outlook Web Access für Exchange 2000 Server finden Sie unter Fehlerbehandlung in Outlook Web Access für Microsoft Exchange 2000 Server.

Copyright

Die in diesem Dokument enthaltenen Informationen entsprechen der zum Zeitpunkt der Veröffentlichung aktuellen Ansicht der Microsoft Corporation bezüglich der behandelten Themen. Da Microsoft auf wechselnde Marktbedingungen reagieren muss, sollte dies nicht als Verpflichtung seitens Microsoft betrachtet werden. Ferner kann Microsoft keine Gewährleistung für die Richtigkeit der dargestellten Informationen nach dem Veröffentlichungsdatum übernehmen.

Dieses White Paper dient nur zu Informationszwecken. MICROSOFT ÜBERNIMMT BEZÜGLICH DER INFORMATIONEN IN DIESEM DOKUMENT KEINE

GEWÄHRLEISTUNGEN, SEI SIE AUSDRÜCKLICH, KONKLUDENT ODER GESETZLICH GEREGELT.

Die Benutzer sind verpflichtet, sich an alle anwendbaren Urheberrechtsgesetze zu halten. Ohne die Urheberrechtsgesetze einzuschränken darf ohne ausdrückliche schriftliche Genehmigung der Microsoft Corporation kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch, mechanisch, durch Fotokopie oder Aufzeichnen, dies geschieht.

Es ist möglich, dass Microsoft Rechte an Patenten bzw.angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Die Bereitstellung dieses Dokuments erteilt keinerlei Lizenzrechte an diesen Patenten, Marken, Urheberrechten oder anderem geistigen Eigentum, ausgenommen, dies wurde explizit durch einen schriftlich festgehaltenen Lizenzvertrag mit der Microsoft Corporation vereinbart.

Die in den Beispielen verwendeten Namen von Firmen, Organisationen, Produkten, Domänennamen, E-Mail-Adressen, Logos, Personen, Orten und Ereignissen sind frei erfunden, soweit dies nicht anders angegeben ist. Jede Ähnlichkeit mit bestehenden Firmen, Organisationen, Produkten, Domänennamen, E-Mail-Adressen, Logos, Personen, Orten und Ereignissen ist rein zufällig und nicht beabsichtigt.

© 2006 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft, MS-DOS, Windows, Windows Server, Windows Vista, Active Directory, ActiveSync, ActiveX, Entourage, Excel, FrontPage, Hotmail, JScript, Microsoft Press, MSDN, MSN, Outlook, SharePoint, Visual Basic, Visual C++, Visual Studio, Win32, Windows Mobile, Windows NT und Windows Server System sind eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern..

Alle anderen geschützten Marken gehören dem jeweiligen Eigentümer.